Analysis of Various Image Steganography techniques

Dr. Amit Chaturvedi
Assistant Prof., MCA Deptt.
Govt. Engineering College, Ajmer
Ajmer, India

Malik Aijaz
M.Phil. Scholar,
Bhagwant University, Ajmer
Ajmer, India

ABSTRACT : Secure data transfer in online communication is bounded due to attacks. Security of data can be achieved by implementing Cryptography and Steganography techniques. Cryptography is an art and science of encryption and decryption of data using key, while as steganography is the art and science of hiding a secret message in a cover media in such a way that no one except the intended recipient knows the existence of the data.All of the existing steganographic techniques use the digital multimedia files as a cover mediums to conceal secret data, but images are the most popular as a cover medium for hiding secret information in images compare to other carrier's file such as text, audio or video. So, there are more possibilities to hide large amount of data inside image file. Hence, the main challenge of the contemporary imagesteganographic system is to embed secret data, which is perceptually indistinguishable, robust and secure such that it is inconspicuous and unaware towards an external observer. JSteg and OutGuessand Hash-LSB with RSA algorithms provide the double to triple security to secret message in a cover image,which is enable to open to the unknown recipient.without the proper information and rules or also can say without the accurate key.In this paper, we are presenting the analysis of various image stagenographytechniquesused for improving the security of secret data.

Keywords: Robustness, Security, Information, Cryptography.

1. INTRODUCTION

The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present. The only missing information for the enemy is the short easily exchangeable random number sequence, the secret key and secure operating system design, a term which refers to all communication paths that cannot easily be restricted by access control mechanisms.The protection of our secret information is primary aim when we want to send some secret information to other. The network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the data privacy and integrity are required to protect against illegal accesses. This has resulted in an expansion of the field of information hiding[1]. Information hiding is the process of hiding the details of an object or function. The hiding of these details results in an abstraction, which reduces the external complexity and makes the object or function easier to use.

Steganography is a way to protect the privacy of valuable information. While cryptography is the process to protecting the secret data by encrypt the content, steganography concerns on protecting the secret message by hiding the content. The concealment of secret messages is achieved by embedding them into other digital mediums as cover [1,2]. Fig.1 shows the Fundamental scheme of stegnography process. In the Embedded section, **a secret message** and a **cover image** (that may be image, video, or audio)is required to hide the secret message. Size of the message cover must be sufficient to hide the secret message. Output of the embedded section is a **stego-image**, which is a modified cover containing secret message. In the recovery section, we need the original message-cover andthe stego-object. Message-cover must be same as used in embedded section. We got the secret message as output of this section by performing some operation which is depending on the technique we use for stegnography.

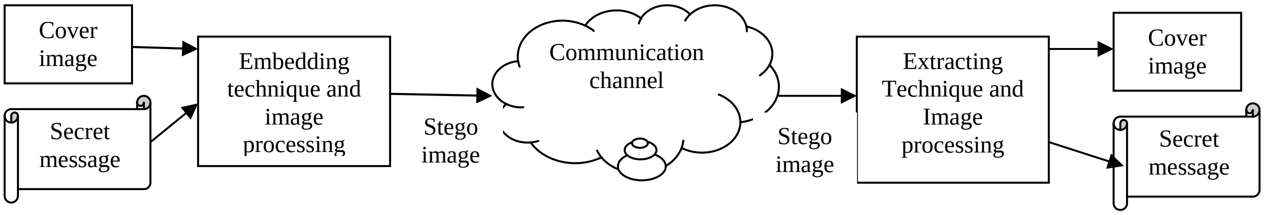

Fig 1 : Basics model for process of Image steganography

2. Techniques for Image Steganography

Steganography is by no means a modern practice. Literally meaning **'covered writing',** it is the practice of hiding messages within other messages cover in order to conceal the existence of the original. Examples of its use can be found throughout history, dating as far back as ancient Greece. However, with the digital media formats in use for data exchange and communication providing abundant hosts for steganographic communication, interest in this practice has increased.The steganography uses the text,images,audio and video as **cover object** to hide the secret message,it means the existence of the one message is concealed in other message for communication on the internet.Here,various techniques of image steganography are presented used for data communication.

(a). Least Significant Bit (LSB) Insertion Steganography

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image [16]. For an 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number [16]. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images).

(b). Random Steganography Technique

The security goals were enhanced via a proposed cryptosystems to maintain the security on the Cover-image. The proposed solution consists of a simple, but strong to hiding the text data and the human eye would be unable to notice the hidden data in the Stego-image. In the message is inserted in the images in random manner in the pixels of a cover image. However, LSB hides the message in a way that the humans do not distinguish it, and still possible for the opponent to retrieve the message due to the simplicity of the technique. Malicious people can easily try to extract the message from the beginning of the image if they are doubtful that there exists secret information that was inserted in the image. Therefore, there is a need to enhance the LSB. New technique is proposed to improve the LSB scheme by inserting the message bit into a set of random in each pixel within the image, not in the least significant bit, and the least significant bit just a sign to extract data from the image. It is proposed in that the inserting of message bits into the image is not only in the least bit but also the other bits in the pixel in the random manner[16]. This can be done by comparing the message bit to the pixel bit randomly chosen from second to the last bit. Based on this comparison, 1 is inserted in the least significant bit if the message bit identical to that of the image, whereas, 0 is inserted if the message bit didn't match with the chosen bit from the image as shown in Table 1.

Pixel Bits	Message Bits	Comparison	Result
1	1	Match	1
0	0	Match	1
1	0	Not match	0
0	1	Not match	0

Table 1 shows Message Bits Comparison

(c). DES Algorithm based steganography

DES encryption (decryption) algorithm takes 8-bit block of plaintext and a 10-bit key to produce an 8-bit ciphertext. The encryption algorithm involves 5 functions: an initial permutation (IP); a complex function fK, which involves both permutation and substitution that depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function fK again and finally, the inverse permutation of IP (IP-1). The function fK takes two 8-bit keys which are obtained from the original 10-bit key.

The 10-bit key is first subjected to permutation (P10) and then a shift operation is performed. The output of the shift operation then passes through permutation function that produces a 8-bit output (P8) for the first sub key (K1). The output of the shift operation again feeds into another shift and (P8) produce the 2nd sub key (K2) [18].We can express encryption algorithm as

Cipher text = IP-1 (fk2 (SW (fk1 (IP (plaintext)))))

K1 = P8 (shift (P10 (key)))

K2 = P8 (shift (shift (P10 (key))))

Plain text = IP-1 (fk 1(SW (fk2 (IP (cipher text)))))

Each byte (pixel) of all the three matrices(R,G,B matrices of payload) are encrypted using DES algorithm and an image comprised of encrypted pixels is formed. The key used to encrypt each pixel is of 10-bit length and is obtained from the pixels of key image.The pixel values of red, green and blue intensities of each pixel of key image are combined to get a 24-bit value. The first ten bits are selected as the key to encrypt the red intensity pixel of payload image. The middle ten bits will be the key to encrypt the green intensity pixel of payload and finally the last ten bits is the key to encrypt blue intensity pixel of payload image. So the size of key image must be same as that of payload. If not, then the key image will get resized. Each pixel (24-bit) of the key image is split into three keys(10- bit each). The encrypted image is embedded within another image called cover-image or carrier image. Cover-image carrying embedded secret image is referred to as stego-image [17].

(d). Hash-LSB with RSA Algorithm based steganography

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure. RSA algorithm procedure can be illustrated in brief as follows [28]:

(i) Select two large strong prime numbers, p and q. Let n = p q.

(ii) Compute Eulerstotient value for n: f (n) = (p - 1) (q - 1).

(iii) Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (n)) = 1.

(iv) Calculate a number d such that d = e-1 mod f (n).

(v) Encryption: Given a plain text m satisfying m < n, then the Cipher text c = m^e mod n.

(vi) Decryption: The cipher text is decrypted by m = c^d mod n.

(e). DNA based Dual Cover Steganography

Dual cover steganography is an evolving technique in the field of covert data transmission. To ameliorate the security of steganography systems we need stronger algorithms as well as new cover media. Recently DNAs are being used as one such cover because of their high information density. Adleman [3], Clell and [4], Leier [5] have done some pioneering work in the field of organic DNA steganography. Despite beinga highly secured technique, DNA steganography algorithms have some common drawbacks like the biological errors (e.g. mutation) and difficulty of implementation. The most feasible solution to this problem is- use of theoretical model of DNAs. By utilizing its natural properties we can strengthen the existing hiding techniques. Some of the

Worth mentioning works are represented here. A combination of cryptography and DNA steganography is utilized in [25], where steganography is used for hidden symmetric encryption key distribution on every new communication. Hayam Mousa *et al. [*26] adopted the reversible contrast mapping technique to develop a reversible information hiding scheme for DNA sequence. Meenakshi S Arya*et al. [*10] proposed a DNA encoding based algorithm to embed watermarks in images with the help of DNA cryptography and spread spectrum watermarking. A secret image is hidden with a cover image by creating 256 in12 proposed a double cover DNA based steganography using magic numbers as the forward tracking algorithm. Suman Chakraborty *et al[11]*. Ithas proposed a loss-less DNA based secret image hiding technique using Sudoku solution matrix. Amal*et al[13]*. Illustrate a DNA-based steganography method combined with a DNA cryptography technique for secure exchange of data in DNA carriers[14]. A secret message is hidden inside a reference DNA strand collected from a publicly available DNA database.Later the indices (locations) of message bases is sent to the Receiver[15]. Dual cover steganography is proposed, in which a theoretical single stranded DNA (ssDNA) is extracted from the pixel information of a cover image[26,27]. The secret message is hidden inside the ssDNA, which in turn is hidden inside the image. During the embedding process the mutated DNA is processed through primer addition, which increases the steganographic security but causes an active mutation to the DNA. This reduces its security against different steganalytic attacks for the cover image. In this paper we propose some of the improvements over the existing model to enhance both its performance and security.

(f). Combination of JSteg and OutGuess algorithms

Steganography is the act of hiding a message inside another message in such a way that the hidden message can only be detected by its intended recipient. We combined two steganography algorithms namely JSteg and OutGuess algorithms, in order to exploit the beneficial characteristics and features of both algorithms to enhance the protection level for secret images. In our proposed approach, the secret message (image) is first concealed inside another image using JSteg algorithm and the resultant stego-image is further hidden inside a final image using OutGuess 0.1 algorithm. In this combine approach, the tricky nature of hiding an already hidden message is usin g two different algorithms increases the level of difficulty for a third party to suspect the existence of a secret image in the first place or even successful decode the it. Besides that, the priority given to the choice of a good image size and type in this approach further discuises the secret image and increases the chances that the image could go unnoticed. Results after calculating the capacity and PSNR for images proved that our approach is a good and acceptable steganography system. The model presented in this approach is based on JPEG images.

3. Related work

The Least Significant Bit (LSB) technique is the most common steganographic technique. An improvement to this technique is suggested by randomly inserting the bits of the message in the image to produce more secured system. The security goals were enhanced via a proposed cryptosystems to maintain the security on the cover-image. The proposed solution consists of a simple, but strong to hiding the text data and the human eye would be unable to notice the hidden data in the Stego-image. The message bits are inserted randomly into the cover-image pixels instead of sequentially. The insertion of message bits into the image is not only in the least bit but also the other bits in the pixel in the random manner[19].

Combination of two steganography algorithms namely JSteg and OutGuess algorithms, in order to exploit the beneficial characteristics and features of both algorithms to enhance the protection level for secret images [20]. The act of hiding an already hidden image (stego image) in another image alone is tricky and deceptive for a third party. Besides that, the idea of combining two steganographic algorithm makes the approach more complex for a third party and this increases the chances that the intended secret massage (secret image) could go unnoticed.Furthermore, in this priority given to selecting a good image sizes and type further disguises the secret image and makes it more difficult for a third party to suspect the existence of a secret image. The experimental results indicated an average PSNR value of more than 50 dB for more than100 images and that is a good and acceptable steganography scheme. The concept of using a theoretical single stranded DNA (ssDNA) as a primary cover, which is extracted from an inconspicuous cover image. In analyzed the security loopholes and performance issues of the existing algorithm and proposed an improved algorithm on the same basis. Performance of both the algorithms are tested against several visual and statistical attacks, and parameterized in termsof both security and capacity. The comparison shows that the proposed improvements provide better overall security. The DNA is attributed by the pixel properties of the image. Thus this procedure makes it more secured than the methods using reference DNAs from public databases. Multiple keys are required for the entire process starting from DNA construction to data embedding, and, their transfer between sender and receiver requires a secure key exchange protocol [21].

Also the new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that’s why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The H-LSB technique have been applied to .tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images [22].

4. Analysis of Image Steganography

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. Embedding a message into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover image. The second file is the message the information to be hidden. A message may be plain-text, cipher-text, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a stego-image. A stego-key (a type of password) may also be used to hide then later decode the message.

To embed the data, the LSB insertion as cited in [23][24] is used. LSB insertion is a common, simple approach in embedding information in a cover file. But in this improved LSB technique, we will insert the data only in last significant byte i.e. blue component of a pixel as that having lowest contribution to the color image according to Human Visual System analysis. To hide a message in a 24-bit image, the B component of each pixel of RGB color image is modified. For example, the letter A can be hidden in a pixel with original data as:(00100111 11101001 11001000). The binary value for A is 01000001. Inserting the binary value for A in the given pixel would result in (00100110 11101001 01000001). The underlined bits are the only actually changed in the bytes used. On average, LSB requires that only half the bits in an image be changed. To hide more data, the cover image should have enough edge pixels to hide the data. Embedding data using 1-3-4 LSB Insertion across Smooth areas To embed the data in smooth areas 1-3-4 LSBs Insertion technique has been utilized which hides data in 1-bit in 1 least significant bit of Red component (Most significant byte),3-bits in 3 least significant bits of Green component and 4 bits in 4 least significant bits of Blue component(Least significant byte) of each selected pixel .This ratio 1:3:4 has been taken depending on their respective contribution of each red, green and blue component to the colors of RGB image.

LSB is a simple approach to embedding information in a cover image.The pixel values of encrypted image is hidden in the lsb of pixels of carrier image by merge it with the 2nd lsb of carrier pixel .If the size of the encrypted image is mxn ,then the size of carrier image must be mxnx8 as each encrypted byte requires 8 bytes (pixels)of carrier image. so if the carrier image size is not eight times the size of the payload , then it has to be resized. In this procedure LSB algorithm helps for securing the originality of image. The extracting is reverse to embedding the encrypted image. In extracting, the carrier image in which the data is hidden is given as an input file.

Here the given image is first encrypted and then the encrypted image is hidden in the carrier image. Finally the hidden encrypted image is decrypted. The Least Significant bit technique by which the encoded bits in the image is decoded and turns to its original state and gives the output as a image. The encryption and decryption in order to secure from unauthorized access. The given below figure 2 demonstrates the mechanism of encryption and decryption.

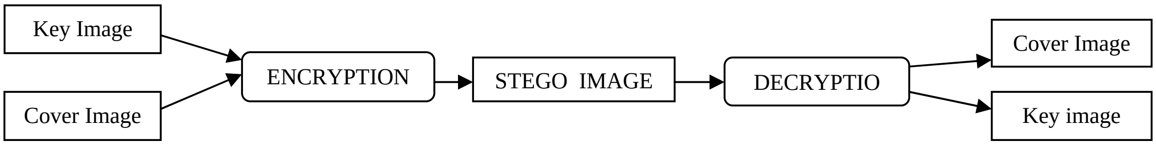

Figure 2 : mechanism of encryption and decryption

To give the double security to the data that we wants to sent to the recipent in valuable or secret form then we can choose another one JSteg algorithm and OutGuess algorithm, to enhance the protection level of hidden images. The secret message (image) is concealed inside an image by using Jsteg algorithm, then the resultant Jsteg-image is again hidden inside another image using OutGuess 0.1 algorithm. The tricky nature of hiding an already hidden image is using two different algorithms introduces some complexity and makes it more deceptive to a third party, hence reducing the suspension of in At the start of this process we take cipher text encrypted from the secret image to be embedded in the cover image.In this process first we converted cipher text into binary form to convert it into bits.Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3,3, and 2 in red,green, and blue channel respectively.The process is continued till entire message of bits will got embedded into the cover image [18]. In the decoding process we have again used the hash function to detect the positions of the LSBs where the data bits had been embedded. When the position of the bits had been specified, the bits are then extracted from the position in the same order as they were embedded. At the end of this process we will get the message in binary form which again converted into decimal form, and with same process we got the cipher text message. After retrieving the positions of LSBs that contain secret data, the receiver will decrypt secret data using RSA algorithm. To apply RSA algorithm receiver will use his/her private key because the secret data have been encrypted by recipient public key. Using receiver private key cipher text will be converted into original message which is in readable form.

5. Conclusion

The basic model for process of image steganography is presented in the figure 1. Combination of two steganography algorithms namely JSteg and OutGuess algorithms, in order to exploit the beneficial characteristics and features of both algorithms are used to enhance the protection level for secret images. The new technique of image steganography is Hash-LSB with RSA algorithm for providing more security to data as well as data hiding method. This technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image.

Acknowledgment

We feel grateful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript.

References

[1] ZaidoonKh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan. O. Alanazi, Overview: Main Fundamentals for Steganography, journal of computing, volume 2, issue 3, march 2010, issn 2151-9617.

the existence of a secret image and significantly enhancingthe protection level.

RSA encryption technique to encrypt the secret data.Encryption includes a message or a file encryption for converting it into the cipher text.Encryption process will use recipient public key to encrypt secret data.It provides security by converting secret data into the cipher text,which will be difficult for any intruder to decrypt it without the recipient private key.

[2] Ashwini Mane, GajananGalshetwar, AmuthaJeyakumar, "DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE" International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

[3] Adleman LM. Molecular computation of solutions to combinatorial problem.*Science* 1994; 266:5187, p. 1021-1024.

[4] Clelland C, Risca V, Bancroft C. Hiding messages in DNA microdots. *Nature* 1999, 399:6736, p. 533-534.

[5] Leier A, Richter C, Banzhaf C, Rauhe H. Cryptography with DNA binary strands. *BioSystems*2000, 57, p. 13-22.

[6] Obaida Mohammad Awad Al-Hazaimeh, ''Hiding Data in Images Using New Random Technique"IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012

[7] HamdanLateefJaheel and ZouBeiji ''A NOVEL APPROACH OF COMBINING STEGANOGRAPHY ALGORITHMS" INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 8, NO. 1, MARCH 2015.

[8]. Torkaman MRN, Nikfard P, Kazazi NS, Abbasy MR, Tabatabaiee SF. Improving Hybrid Cryptosystems with DNA Steganography. *DEIS 2011*, p. 42-52, 2011.

[9]. Mousa H, Moustafa K, Abdel-Wahed W, Hadhoud M. Data Hiding Based on Contrast Mapping Using DNA Medium. In: *The International Arab Journal of Information Technology*, 8:2, p. 147-154, 2011.

[10]. Arya MS, Jain N, Sisodia J, Sehgal N. DNA Encoding Based Feature Extraction for Biometric Watermarking. In: *International Conference on Image Information Processing (ICIIP 2011)*, 2011.

[11]. Bandyopadhyay SK, Chakraborty S. IMAGE STEGANOGRAPHY USING DNA SEQUENCE. In: *Asian Journal Of Computer Science And Information Technology*, 1:2, p. 50-52, 2011.

[12]. Chakraborty S, Bandyopadhyay SK. Two Stages Data-Image Steganography Using DNA Sequence. In: *International Journal of Engineering Research and Development*, 2:7, p. 69-72, August 2012.

[13]. Chakraborty S, Roy S, Bandyopadhyay SK. Image Steganography Using DNA Sequence and Sudoku Solution Matrix. In: *International Journal of Advanced Research in Computer Science and Software Engineering*, 2:2, February 2012.

[14]. Khalifa A, Atito A. High-Capacity DNA-based Steganography. In: *The 8th International Conference on INFOrmatics and Systems (INFOS2012)*, Bio-inspired Optimization Algonthms and Their Applications Track, May 2012.

[15]. Abbasy MR, Nikfard P, Ordi A, Torkaman MRN. DNA Base Data Hiding Algorithm. In: *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, 2:1, p. 183-192, 2012.

[16] Dr.EktaWalia, PayalJainb, Navdeep, "*An Analysis of LSB & DCT based Steganography*", Global Journal of Computer Science and Technology, Vol. 10, Issue No. 1, April, 2010.

[17] R.Nivedhitha1, Dr.T.Meyyappan,'' Image Security Using Steganography And Cryptographic Techniques''*International Journal of Engineering Trends and Technology- Volume3Issue3- 2012*

[18] KousikDasgupta, J. K. Mandal, ParamarthaDutta, "*Hash Based Least Significant Bit Technique for Video Steganography (HLSB)*", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[19] Obaida Mohammad Award Al-Hazaimeh'' Hiding data in images using new Random Technique'' *International Journal of computer sciences-vol 9 issue 4,No. 2,july 2012.*

[20] HamdanLateefJaheel,ZouBeiji,.''A Novel Approach Of Combining SteganogrphyAlgorithm*''international journal on smart sensing and intelligent systems'', vol 8,No.1 ,March 2015.*

[21] Prasenjit Das , SubhrajyotiDeb,NirmalyaKar, Baby Bhattacharya,''An Improved DNA based Dual Cover Steganography'',*''international conference on information and communication Technologies(ICICT-2014).*

[22] Anil Kumar ,Rohini Sharma,'' A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique'''' *international journal of Advanced Research in Computer Science and Software Engineering''.vol 3,issue 7,July 2013*

[23] M. Juneja and P. S. Sandhu, "Designing of robust image steganography technique based on LSB insertion and encryption," presented at the International Conference on Advances in Recent Technologies in Communication and Computing (ARTCOM-2009), Kerala, India, October 27-28, 2009.

[24] Data Encryption Standard (DES), National Bureau of Standards (US), Federal Information Processing Standards Publication National Technical information Service. Springfield VA. April 1997.

[25] Torkaman MRN, Nikfard P, Kazazi NS, Abbasy MR, TabatabaieeSF.Improving Hybrid Cryptosystems with DNA Steganography.DEIS 2011,p. 42-52,2011.

[26] .Das P ,Kar N. A DNA Based image Steganography Using 2D Chaotic Map. In: proceedings of International Conference on Electronics and Communication Systems(ICESS-2014) , P, 149-153 , 13th – 14February ,2014.

[27] Das P,Kar N. A Highly Secure DNA Based Image Steganography .In :IEEE International Conference on Green Computing , Communication And Electrical Engineering (ICGCCEE'14), 6th-8th March,2014.

[28] Chandra.M.Kota, CherifAissi, "*Implementation of the RSA algorithm and its cryptanalysis"*, ASEE Gulf-Southwest Annual Conference, American Society for Engineering Education, USA, 2002.

AUTHORS PROFILE

Dr. AmitKumar Chaturvedi, Assistant Prof., MCA Deptt., Govt. Engineering College, Ajmer have completed Ph.D. (Computer Sc.) in Mar, 2012. He has more than 15 years of teaching experience. He have published around 38 research papers in national and international Journals in the area of Mobile computing system, Spectrum requirement estimation for 4G, and Cryptography and always ready to teach the subjects to his students, which he does with great finesse.

Malik Aijaz received the bachelors degree (with Information Technology) from University of Kashmir, Srinagar, India in 2011. He received the M.Sc.(IT) degree from HNB Garhwal University, Srinagar (Garhwal) Uttarakhand in Jully 2014. He ispresently a research scholar in M.Phil.(IT), Bhagwant University, Ajmer. His research interests include Steganography.