Hybrid algorithms for Secure Encrypted Data Hiding Technique: A Survey

Naveen Jain*, Kailash Patidar and Narendra Sharma*****
**Department of (CSE), Student, M Tech IV Semester, SSSIST, RGTU, Bhopal, India*
naveen.jain01@gmail.com
***HOD CSE, SSSIST, RGTU, Bhopal, India*
Kailashpatidar123@gmail.com
****Assistant professor, CSE, SSSIST, RGTU, Bhopal, India*
narendra_sharma88@gmail.com

Abstract: **The data security and its authenticity is an important area of research, where the daily real time world scenario demands a secure and authentic communication in between different agencies. Data protection and sharing using latest trend is always a research of study. Different authors in papers described a hybrid approach which take combination of encryption and then perform hiding it before transmission, thus an intruder required to break encryption and steganography policy to grab the original data. In this paper our contribution is to survey different available technique with support such combination and their impact on security. Also the work illustrate the further enhancement can be done to obtain maximum security of data over the communication message.**

Keywords: **data authenticity, encryption over data, data hiding, multi-level approach.**

INTRODUCTION

Information hiding is a science which dates back to 1499, and it has long history. It has been used in various forms for 2500 years. It has found use in military, diplomatic, personal, spies, ruler, governments etc. Steganography has been widely used, including in recent historical times and the present day. Some known examples include: Past Early steganography was messy. Before phones, before mail, before horses, messages were sent on Foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger. While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times. - according to Greek historian Herodotus, the famous Greek tyrant Histiaeus while in prison, used unusual method to send message to his son in- law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in-law. Herodotus provides the first records of steganography in Greece [13]. - to communicate Greeks would etch the message they wished to send into the wax. - coating of a wooden tablet. The tablet would then be transported to the recipient who would read the message, then re-melt the wax to etch their reply. In order to communicate in secret, the army would remove the wax completely, carve thesecret message into the wood, and re-coat the tablet with wax [13]. - Messages were also written on envelopes in the area covered by postage stamps to avoid the possible detection of the message. Present In today's generation, as most of the people often transmit images, audio over the internet, so most of the Steganographysystem's uses multimedia objects like image, audio and video as cover sources to hide the confidential data [14]. So, on the basis of this, steganography is divided into four categories: Text Steganography, Image Steganography, Audio/VideoSteganography Protocol Steganography. Future Strength analysis can be defined as process to crack the cover object in order to get the hidden data. In general terms, it is known as Hacking i.e. unauthorized access of data during transmission. Future perspective of steganography lies on combining steganography with cryptography to achieve a higher level of security such that even if intruder detects the hidden message, he/she will not be able to decode it.

LSB (Least Significant Bit) method [8] It is a standout amongst the most well-known and least demanding techniques for message covering up. In this system, message is covered up at all critical bits of picture pixels .Changing the LSB of the pixels does not present much distinction in the picture and in this way the steno picture appears to be like the first picture. In the event of 24- bit pictures three bits of pixel can be utilized for LSB substitution as every pixel have separate parts for red, green and blue.

LITERATURE REVIEW

In [3] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range

indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

in [4] proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited; there is not a single image which has many edges with noise region like 'Baboon.tif'.

In [5] authors have proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSB's of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (MxN) pixels.

In [11] proposed an image steganographic method of mapping pixels to alphabetic letters. It maps the 32 letters (26 for English alphabetic and other for special characters) with the pixel values. Five (5) bits are required to represent these 32 letters and authors have generated a table where 4 cases design to represent these 32 letters. According to that table, each letter can be represented in all 4 cases. It utilizes the image 7 MSB (Most Significant Bits) (27 = 128) bits for mapping. Proposed method maps each 4-case from the 7 MSB's of pixel to one of the 32-cases in that table. These 4-cases increase the probability of matching. This algorithm keeps the matching pattern of cover-image which is then used for extracting data from the stego-image. Proposed method does not required any edge or smoothness computations but secret data should be in the form of text or letter for embedding.

In Paper [15]," A Symmetric Key Encryption Technique Using Genetic Algorithm Key"In this paper author proposed a genetic algorithm based symmetric key cryptosystem for encryption and decryption , here the plain text and the user input is converted into text matrix and key matrix respectively . an additive matrix is generated by adding the text matrix and key matrix . a linear substitution function is applied on an additive matrix to produce the intermediate cipher. Then the GA functions (crossover and mutation) are applied on the intermediate cipher to produce the final cipher text. Genetic algorithm is secure since it does not utilize the natural numbers directly .in this paper author use two point crossover techniques and flipping of bits mutation technique. author stated that symmetric key substitution algorithm is used to ensure confidentiality in networks which is combined and implemented with the help of genetic algorithm function to provide added security.

In this paper author[16] proposed an efficient security model in computing environment with the help of soft computing techniques . here a strong security in cloud computing is managed with the help of reputation management system to ensure the data security . also maintaining the transaction table that contains the info. Related to the previous transaction like the previous transaction ID of the cloud node involved , timestamp, public keys of the cloud involved , trust evaluation etc. Can be very helpful to identify the relevant cloud nodes suitable of data transmission. In this method author utilized genetic algorithm as the computing technique to identify the suitable nodes for transmission that proved to be effective method in cloud computing environment and provide security to the cloud system.

Cornwell [17] talked about the outline of Bruce Schneider's Blowfish encryption calculation alongside an execution investigation what's more, conceivable assaults. It was finished up about the viability of Blowfish with the other surely understood calculations DES, 3DES, and AES. It was presumed that Blowfish can give long haul information security with no known secondary passage powerlessness or capacity to diminish the key size. For the future

degree Blowfish was viewed as sheltered and powerful plan albeit future re-examinations will be required.

PROBLEM FORMULATION

As per analysis of different encryption and steganography technique the algorithm is further having some problem in combination where the enhancement is further required to contribute, the points are:

1. A combination can be generating where the key for the data hiding can be generate using some algorithm approach.
2. In LSB technique different variant can be utilize to make visual effect as it , such case R LSB , E LSB technique can be used which provide better vision for the image content.
3. Determining the encryption combination to get maximum avalanche effect value than existing approach.
4. To obtain encryption that provide large encryption key to regain the original data.

PROPOSED WORK

The work discussed in literature contains the different approach for data security which increase the key length and provide the data security, the further approach can apply to enhance LSB to E LSB technique for the proposed work along with the symmetric key encryption technique which provide the high resolution with low computation time for the encryption and decryption as compare to other approach. Thus a symmetric key encryption and E-LSB approach can be further develop to maximize the security.

In ELSB, we use all the edge pixels in an image. Here, we first calculate the masked image by masking the two LSB bits in the cover image. Then we identify the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels we hide the data in the LSB bits of the edge pixels only and send the stego object to the receiver. At the receiver, the stego object is again masked at the two LSB bits. Then the canny edge detector is used to identify the edge pixels. We will get same edge pixels at the sender and receiver since we used the same masked image to calculate the edge pixels. Thus we identify the bits where data is hidden.

CONCLUSION

In this paper the discussion is done with the different approach which provides effective security using cryptography and steganography concept. The different cryptographic technique provide high security on providing good key length also further security is combined with steganography approach which is used to hide the encrypted data. Thus in order to reverse a cycle intruder will require two key phase. As per our analysis the combine approach always required a great effort and complexity to decode the message, thus the approach is suitable for any data security approach in application area such as army, intelligence etc.

REFERENCES

[1]. Md. Rashedul Islam1, Ayasha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. DelowarHossain "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" IEEE 2014.

[2]. Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, **(2010)** March 1.

[3]. H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radio engineering, vol. 18, no. 4, **(2009)**, pp. 509-516.

[4]. S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, **(2009)**.

[5]. C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[6]. K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), **(2008)** August 28-30, pp. 355-358.

[7]. H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on **(2009)** May.

[8]. W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, **(2010)** April 4.

[9]. V. MadhuViswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, **(2010)**.

[10]. M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, vol. 5, no. 1, **(2009)**, pp. 33-38.

[11]. H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, **(2007)**.

[12]. B. Ahuja, M. Kaur and M. Rachna, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, vol. 1, no. 1, **(2009)** May.

[13]. M. TanvirParvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, **(2008)**, pp. 1322-1327.

[14]. A. M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, **(2009)**.

[15]. Awsnaserjaber,mohamadfadli bin zolkipli,2013, "use of cryptography in cloud computing".

[16]. Vijay .g.r , a. Rama mohan reddy,2012, "an efficient security model in cloud computing based on soft computing techniques.

[17]. Tamimi A. Al., "Execution Analysis of Data Encryption Algorithms", Oct 2008.

