INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

A SURVEY ON SECRET MESSAGE HIDING TECHNIQUES USING SYMMETRIC CRYPTOGRAPHY

Shailja Sharma[1*] and Prof. Sanjeev Acharya[2]

[1]M.Tech. Scholar MIT, Bhopal, shailjasharma1990@gmail.com

[2]Prof. CSE Dept, MIT, Bhopal

E.mail: sshailja116@gmail.coms.acharya@gmail.com

Abstract

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called Steganography. steganography is the art and science of invisible communication as we mentioned in abstract part. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information..it is important phenomenon to secure the message data.

Keyword: - Cryptography,Image, Steganography,Encryption,Decryption Etc.

Introduction

With worry of time, classification or secreteness has dependably been critical. Regardless of whether it is composed on archive or sends over the Internet, engraved in stone, correspondence between two clients is uncovered to spying. In this way, it is important to show a system that secures such kind of data. A standout amongst the most utilize full and regular strategies of securing transmitted data is cryptography. The reason for cryptography is to cover discernable content such that it progresses toward becoming un-lucid content. This is known as figure content would then be able to be safely and securely transmitted to another end or goal end. Knowing the strategy is utilized for encryption, where just the collector client will be fit to get the first message. Access to intense PCs improves encryption. It can similarly be an instrument utilized for breaking a figure or unscrambling a message. Regardless of how effective the encryption calculation is, scrambled information will dependably stir doubt [3]. This is the place steganography method can offer assistance. Steganography strategy can be characterized as "the craftsmanship with art of imparting in a way which conceals the presence of correspondence" [2]. Despite the fact that cryptography and steganography are regularly puzzled, they are basically extraordinary. While the first "scrambles a message so it can't be comprehended", the other one "shrouds the message so it can't be seen" [1]. It is normally accepted, erroneously, that steganography could supplant cryptography. Unexpectedly, by utilizing the two strategies together one can make a strong and effective encryption framework, superior to each of the two segments. On the based of such hypothesis proposed work is additionally introducing a solid idea for the security of the data whatever content or picture over web in this work where steganography procedure and cryptography system are worked with together to give security of every strategy exclusively in consolidated way.

The process of information hiding may involve the following concepts:

A-Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio and video as well as file structures, and html pages to name a few.

B-Stego-object: refers to the object which is carrying a hidden message. So given a cover object, and a message the goal of the steganographer is to produce a stego-object which would carry the message.

1.1 RELATED WORK

In [1] a multi secure and power of restorative picture based steganography conspire is proposed. This proposed strategy gives a productive and capacity security component for the insurance of computerized medicinal pictures. In this Integer Wavelet Transform (IWT) is utilized to secure the MRI restorative picture into a solitary holder picture. The compartment picture was taken and flip left was connected and the fake holder picture was acquired. At that point the patient's therapeutic conclusion picture was taken as mystery picture and Arnold change was connected and mixed mystery picture was acquired. In the principal case, the mixed mystery picture was installed into the fake holder picture and Inverse IWT was taken to get a fake mystery picture. In the second case, the compartment picture was brought and combined with the fake mystery picture and stego picture was gotten. In [2] is worried about executing Steganography for pictures, with a change in both security and picture quality. The one that is actualized here is a variety of plain LSB (Least Significant Bit) calculation. The stego-picture quality is enhanced by utilizing bit-reversal method. In this procedure, certain slightest huge bits of cover picture are upset after LSB steganography that co-happen with some example of different bits and that lessens the quantity of altered LSBs. Accordingly, less number of minimum critical bits of cover picture is changed in contrast with plain LSB technique, enhancing the PSNR of stegoimage. By putting away the bit designs for which LSBs are upset, message picture can be gotten accurately. To enhance the heartiness of steganography, RC4 calculation has been utilized to accomplish the randomization secluded from everything message

picture bits into cover picture pixels as opposed to putting away them consecutively. This procedure haphazardly scatters the bits of the message in the cover picture and along these lines, making it harder for unapproved individuals to separate the first message. To maintain a strategic distance from the commotion mutilation in the picture, the LSB addition technique is utilized to embed the bits in a picture by utilizing irregular number generators. In [3] exhibited system before installing the mystery data into a picture, the mystery data has been compacted utilizing the wavelet change procedure. The got bits after pressure are encoded utilizing quantum doors. In [4] the proposed work shows a remarkable system for Image steganography in light of the Data Encryption Standard (DES) utilizing the quality of S-Box mapping and Secrete key. The preprocessing of emit picture is conveyed by implanting capacity of the steganography calculation utilizing two one of a kind S-boxes. The preprocessing give abnormal state of security as extraction is unrealistic without the learning of mapping rules and emit key of the capacity. Furthermore the proposed conspire is equipped for not simply scrambling information but rather it likewise changes the force of the pixels which adds to the wellbeing of the encryption. In [5] I have investigated that creator proposes three indigenous strategies as a variation of Cipher Block Chaining (CBC) mode for picture encryption by considering three diverse crossing way (Horizontal, Vertical and Diagonal). In strategy one basic Raster Scan has been utilized to scramble the secret Image called Horizontal Image Scrambling (HIS). Strategy two is a variation of technique one called Vertical Image Scrambling (VIS), here crossing way would be start to finish left to Right. Third technique utilizes corner to corner navigating way called Diagonal Image Scrambling (DIS). Later Image Steganography has been adjusted to send these Scrambled Images in an unnoticeable way. In [6] mystery sharing alludes to a strategy for disseminating a mystery among a gathering of members, each of whom is apportioned with an offer of the mystery. The member's offers are utilized to remake the mystery. Single individual members share is of no utilization. The reversible picture sharing methodology and edge plans are utilized accomplish the novel mystery shading picture sharing. The mystery shading picture pixels will be changed to m-ary notational framework. The reversible polynomial capacity will be created utilizing (t-1) digits of mystery shading picture pixels. Mystery shares are produced with the assistance of reversible polynomial capacity and the member's numerical key. The mystery picture and the cover picture is inserted together to build a stego picture. The reversible picture sharing procedure is utilized to remake the mystery picture and cover picture. The mystery is acquired by the lagrange's equation created from the adequate mystery shares. Quantization prepare is connected to enhance the nature of the cover picture. Pinnacle flag to commotion proportion is connected to break down the nature of the stego pictures. The recreation comes about demonstrate that the mystery and cover are reproduced without misfortune [6]. Security, the most well-known word expressed by any man, any gadget, any fringe since recent hundreds of years. Security from malignant sources has turned into a piece of the innovation or the disclosure cycle. Bunch techniques for assurance are utilized running from a basic confirmation secret word to most cryptography calculations for securing the outrageous delicate or private information. In [7] an instructional exercise audit of the steganography procedures showed up. Different picture steganography strategies have been proposed. In this I research of established steganography methods and steganalysis strategies. I express an arrangement of criteria to break down and assess the qualities and shortcomings of the past procedures. The minimum critical piece (LSB) addition technique is the most widely recognized and least demanding strategy for implanting messages in a picture with high limit, while it is perceivable by factual investigation, for example, RS and Chi-square examinations. In [7] creators propose a novel LSB picture steganography calculation that can viably oppose picture steganalysis in light of measurable analysis.In [8] I have watched that creators propose an approach for Image steganography in light of LSB utilizing X-box mapping where they have utilized a few Xboxes having interesting information. The installing part is finished by Steganography calculation where they utilize four one of a kind X-boxes with sixteen distinct esteems (spoken to by 4-bits) and each esteem is mapped to the four LSBs of the cover picture. This mapping gives adequate security to the payload in light of the fact that without knowing the mapping rules nobody can extricate the mystery information (payload). The development of fast PC systems and that of the Internet, specifically, has expanded the simplicity of Information Communication. Amusingly, the reason for the advancement is additionally of the misgiving - utilization of computerized arranged information. In correlation with Analog media, Digital media offers a few unmistakable focal points, for example, high caliber, simple altering, high devotion duplicating, pressure and so on. In any case, this sort progression in the field of information correspondence in other sense has climbed the dread of getting the information snooped at the season of sending it from the sender to the collector. Along these lines, Information Security is turning into an indistinguishable piece of Data Communication. Keeping in mind the end goal to address this Information Security Steganography assumes an imperative part. Steganography is the workmanship and art of composing shrouded messages such that nobody separated from the sender and proposed beneficiary even acknowledges there is a concealed message. In [9] we have watched that a strategy for picture steganography in view of Huffman Encoding is introduced. In which two 8 bit dim level picture of size M X N and P X Q are utilizing as a cover picture and mystery picture individually. Huffman Encoding is performing over the mystery picture/message before inserting and each piece of Huffman code of mystery picture/message is implanted inside the cover picture by modifying the minimum huge piece (LSB) of each of the pixel's powers of cover picture. The span of the Huffman encoded bit stream and Huffman Table are additionally installing inside the cover picture, so that the Stego-Image moves toward becoming independent data to the recipient. Picture steganography is a strategy for hiding data into a cover picture to shroud it. Minimum Significant-Bit (LSB) based approach is most well known steganographic methods in spatial space because of its straightforwardness and concealing limit. In [10] communicated a novel calculation of information concealing utilizing cryptography named as ASK calculation. Touchy information is hided in a shading picture utilizing cryptography. This shows how information can be send utilizing a shading picture without obliviousness of outsider. Calculation portrayed a technique for vanishing information in a shading picture. In

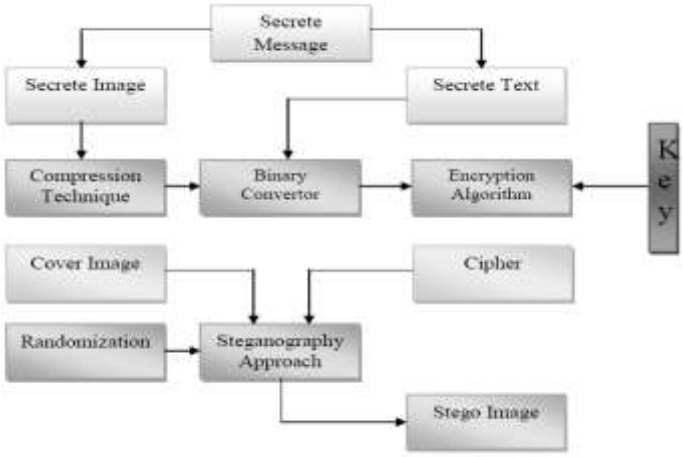
[11] concentrated on the mix of cryptography and steganography strategies and another method – Metamorphic Cryptography has recommended. The message is changed into a figure picture utilizing a key, hidden into another picture utilizing steganography by changing over it into a middle content lastly changed by and by into a picture. The intricacy of cryptography does not enable many individuals to really comprehend the inspirations and along these lines accessible for honing security cryptography. Cryptography prepare tries to circulate an estimation of essential cryptographic primitives over various intersections keeping in mind the end goal to decrease security suspicions on singular hubs, which build up a level of adaptation to non-critical failure restricting to the hub modification. In a continuously arranged and disseminated correspondences condition, there are an ever increasing number of valuable circumstances where the capacity to convey a calculation between various dissimilar to organize convergences is required. The reason back to the effectiveness (isolate hubs perform unmistakable errands), adaptation to non-critical failure (if a few hubs are inaccessible then others can play out the assignment) and security (the trust required to play out the undertaking is shared between hubs) that request in an unexpected way.

1.2 PROPOSED SOLUTION

Security is the prime worry amid data (Text, Image) going over web. With this proposed work are exhibiting a security idea where cryptography and steganography consolidated together to full fill the necessity of solid security of the data (Text, Image) over web. In the proposed idea cryptography give encryption/unscrambling idea where steganography give data (Text, Image) concealing idea that mean proposed idea has two level of security. Figure 1.1 is demonstrating the general perspective of proposed idea where a mystery message gone through proposed encryption handle where it change over into garbled shape known as figure emit message. On the off chance that the emit message is content at that point there is no issue to deal with it yet discharge message is picture then its definitely known a picture have expansive in estimate so there is issue to deal with substantial information measure with high proficiency. With the goal that proposed idea are utilizing picture examination procedure to lessened the extent of the emit picture to simple deal with. In both case (content, picture) discharge message are change over itself into double esteem and tese twofold esteem are work with encryption handle where encryption prepare are utilizing an extraordinary incentive for the security object is known as key esteem. This key esteem is private and just shared amongst sender and recipient through private channel. In the wake of finishing encryption prepare delivered figure message are passed to steganography method where a cover picture will likewise go to steganography strategy. To give greater security in steganography proposed idea are likewise apply randomization in steganography strategy that mean there is another uncommon esteem are utilizing as a randomization which is giving extra security to steganography and created stego picture.

.

Solution View Architecture



1.3 PERFORMANCE METRICS

PSNR: Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation

Correlation : Correlation is a statistical measure that indicates the extent to which two or more variables fluctuate together.

Entropy: Image entropy is a quantity which is used to describe the `business' of an image, i.e. the amount of information which must be coded for by a compression algorithm.

Key: Secret snippet of data, for example, pwd, distinguishing proof number, advanced endorsement and so forth utilized as a part of conjunction with calculation to scramble information or document. To scramble a record you require a calculation and a key, to unscramble an information you likewise require a calculation and a key. The key may, or may not be the same for record encryption

CONCLUSION

This research study utilized a new algorithm to embed a text message in a gray image using a random key. The hiding process included concealing the plain text using column by column technique. The results demonstrated by the above

table showed that a high level of security was achieved and the quality of the image was preserved. This research project did not take into account an image that contains noise which could be considered a direction for future work.

.

REFERENCES

[1] Sujarani Rajendran, Manivannan Doraipandian *"Chaotic Map Based Random Image Steganography Using LSB Technique"*, International Journal of Network Security, Vol.19, No.4, PP.593-598, July 2017

[2] G Prabakaran, R. Bhavani, P.S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013 , Page(s): 1188 – 1193

[3] M.K Ramaiya. ; N.Hemrajani, ; , A.K Saxena. "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013 , Page(s): 1094 - 1099

[4] N. Akhtar, ; P. Johri, ; S Khan, "Enhancing the Security and Quality of LSB Based Image Steganography" 5th International Conference on Computational Intelligence and Communication Networks (CICN), Publication Year: 2013 , Page(s): 385 – 390

[5] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[6] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012

[7] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[8] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

[9] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[10] Thomas Leontin Philjon. and Venkateshvara Rao. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[11] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[12] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE

[13] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

[14] Mohit Kulkarni, Maitreyee Phatak, Uma Rathod, Sudhir Prajapati, Mrs. Shivganga Mujgond *"Efficient Data Hiding Scheme Using Audio Steganography"*, International Research Journal of Engineering and Technology (IRJET), Mar-2016

[15] Manoj Kumar, Naveen Hemrajani and Anil Kishore Saxena "Security Improvisation in Image Steganography using DES" IEEE 2012

[16] Sesha Pallavi Indrakanti , P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[17] Qais H. Alsafasfeh , Aouda A. Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems Journal of Signal and Information Processing, 2011.

[18] M.J.Thenmozhi, Dr.T.Menakadevi *"A New Secure Image Steganography Using Lsb And Spiht Based Compression Method"*, International Journal of Engineering Research & Science (IJOER), 2016

[19] Amnesh Goel, Reji Mathews, Nidhi Chandra "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices" International Journal of Computer Applications (0975 – 8887) Volume 36– No.3, December 2011.

[20] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, Image Encryption Using Affine Transform and XOR Operation ,International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[21] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption "2010 IEEE International Conference on Electronics and Information Engineering (ICEIE 2010)

[22] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping, DAI Wei-di "Digital Image Encryption Algorithm Based on Chaos and Improved DES" "Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009

[23] 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

[24] Nada ElyaTawfiq "Hiding Text within Image Using LSB Replacement" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 (Jul. - Aug. 2013)

[25] Hyder Yahya Atown "Hide and Encryption Fingerprint Image by using LSB and Transposition Pixel by Spiral Method" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014