Volume 2 Issue 2 | June 2014 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Review on Novel Steganography Approach using Cryptography

Mukta Bhatele
Professor & Head
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P.) [INDIA]
Email:mukta_bhatele@rediffmail.com

Megha Tiwari
M-Tech Scholar
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P.) [INDIA]
Email: er.meghatiwari@gmail.com

Vigyan Sharma
Assistant Professor
Department of Computer Science and Engineering
Jai Narain College of Technology,
Bhopal (M.P.) [INDIA]
Email: vigyan.sharma@yahoo.co.in

Abstract**—***We have already known that cryptography technique provided ideal or harmless security. Cryptography technique is also used to achieve various security principal like integrity, un-authorization, confidentiality and many more. Proposed Security system is also based on these security principal and trying to full fill basic requirement of security through design and developed double layer of security for image information. Proposed security system, when it's properly design and developed, makes attempts to brawny security cost-excessive. The proposed research, analyze the combine principle of the steganography and cryptography technique. Moreover the Performance with security of the proposed security system is also evaluated. The Obtainable results based on the proposed concept which is combined technique of steganography as well as cryptography appreciative the efficiency of the proposed security system, and the combination of steganography technique with cryptography technique illustrate higher security.*

Keyword:—*Steganography, Security, Encryption, Decryption, Internet*

1. INTRODUCTION

Today in digital world the medium of transmitting of the information via internet and there are lots attacker to captured the information because the information has transferred through hidden channels. Cryptography technique used principal like integrity, un-authorization, confidentiality and many more. Proposed Security system is also based on integrity, un-authorization, confidentiality and trying to full fill basic requirement of security through design and developed double layer of security for image information. When proposed security system is properly design and developed, makes attempts to jacked security cost-excessive. Combination of symmetric cryptography and steganography technique to take benefit of the each type of security technique. Symmetric encryption has the performance advantage and therefore is the common solution for encrypting and decrypting performance-sensitive data, such as an online data stream. However, symmetric encryption has a downside the cryptographic key needs to be known to both the sender and

receiver of encrypted data, and the exchanging of the key over an insecure channel may cause security risks.

2. RELATED WORK

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data [9].

In [2] embedded huge amount of secret information using LSB technique. To achieve this first the secret information is compressed using wavelet transforms. After compression the bits are encoded using a reversible quantum gate. LSB is one of the best techniques when compared to transformation techniques, because it reduces lots of noise distortion.

In [4] the proposed work presents a unique technique for Image steganography based on the Data Encryption Standard (DES) using the strength of S- Box mapping & Secrete key. The preprocessing of secrete image is carried by embedding function of the steganography algorithm using two unique S-boxes. The preprocessing provide high level of security as extraction is not possible without the knowledge of mapping rules and secrete key of the function. Additionally the proposed scheme is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

In [5] we have observed that a technique for image steganography based on Huffman Encoding is presented. In which two 8 bit gray level image of size M X N and P X Q are using as a cover image and secret image respectively. Huffman Encoding is performing over the secret image/message before embedding and each bit of Huffman code of secret image/ message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedding inside the cover image, so that the Stego-Image becomes standalone information to the receiver. Image steganography is a method of concealing information into a cover image to hide it. Least Significant-Bit (LSB) based approach is most popular steganographic techniques in spatial domain due to its simplicity and hiding capacity.

In [6] presented an approach for Image steganography based on LSB using X-box mapping where they have used several Xboxes having unique data. The embedding part is done by Steganography algorithm where they use four unique X-boxes with sixteen different values (represented by 4-bits) and each value is mapped to the four LSBs of the cover image. This mapping provides sufficient security to the payload because without knowing the mapping rules no one can extract the secret data (payload).

In [7] presented three indigenous methods as a variant of Cipher Block Chaining (CBC) mode for image encryption by considering three different traversing path (Horizontal, Vertical and Diagonal). In method one simple Raster Scan has been employed to scramble the confidential Image called Horizontal Image Scrambling (HIS). Method two is a variant of method one called Vertical Image Scrambling (VIS), here traversing path would be top to bottom left to Right. Third method employs diagonal traversing path called Diagonal Image Scrambling (DIS). Later Image Steganography has been adapted to send these Scrambled Images in an unnoticeable manner.

In [8] the reversible image sharing approach and threshold schemes are used in this concept to achieve the novel secret color image sharing. The secret color image pixels will be transformed to m-ary notational system. The reversible polynomial function will be generated using (t-1) digits of secret color image pixels. Secret shares are generated with the help of reversible polynomial function

and the participant's numerical key. The secret image and the cover image is embedded together to construct a stego image. The reversible image sharing process is used to reconstruct the secret image and cover image. The secret is obtained by the lagrange's formula generated from the sufficient secret shares. Quantization process is applied to improve the quality of the cover image.

In [9] describes an edge adaptive image stenographic scheme in the spatial LSB domain they usually exists some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. To preserve the statistical and visual features in cover images, presented scheme which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges.

In [15] expressed a novel algorithm of data hiding using cryptography named as ASK algorithm. Sensitive data is hided in a color image using cryptography. This shows how data can be send using a color image without ignorance of third party. Algorithm described a method for vanishing data in a color image.

In [16] focused on the combination of cryptography and steganography methods and a new technique – Metamorphic Cryptography has suggested. The message is transformed into a cipher image using a key, concealed into another image using steganography by converting it into an intermediate text and finally transformed once again into an image. The complexity of cryptography does not allow many people to actually understand the motivations and therefore available for practicing security cryptography. Cryptography process seeks to distribute an estimation of basic cryptographic primitives across a number of confluences in order to reduce security assumptions on individual nodes, which establish a level of fault-tolerance opposing to the node alteration. In a progressively networked and distributed communications environment, there are more and more useful situations where the ability to distribute a computation between a number of unlike network intersections is needed. The reason back to the efficiency (separate nodes perform distinct tasks), fault-tolerance (if some nodes are unavailable then others can perform the task) and security (the trust required to perform the task is shared between nodes) that order differently.

Hence, in [17] described and reviewed the different research that has done toward text encryption and description in the block cipher. Moreover, in this suggests a cryptography model in the block cipher. There are many security issues in data communication. Cryptography is a substantially safe method to provide protection in data receiving and sending.

3. EXISTING ISSUES

From the study of the previous research there are many points are noticed that can make un-efficient or imperceptibility of an algorithm.

Efficiency: efficiency of the algorithm that means how much efficient in terms of time and how much efficient in terms of memory. Time and memory both are play an important role in efficiency.

Security: Security is the prim concerned in the field of encryption. It known that information over public network should be highly secured otherwise any eavesdropper can be easily access information. Encryption Key is play an important role in the field of encryption and security of the algorithm is depending upon key length. Higher key length will be causes higher security.

Throughput: we can define throughput as "total size of plain text divide by total execution time during encryption/decryption". Execution speed can be measured by throughput.

Throughput = (Size of plain Text to be Encrypt/ Total Execution Time during Encryption) … (1).

Error- Rate: "Error find per execution" that means in single execution how much error have noticed. Minimum error denoted efficient algorithm.

Bandwidth: In computer networking and computer science, the words bandwidth, network bandwidth, data bandwidth, or digital bandwidth are common. Here I am focusing on data bandwidth. Data bandwidth is the amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second.

Secrecy: The secrecy of existing algorithm is the first and foremost requirement, since the strength of existing algorithm lies in its ability to be unnoticed by the human eye. The moment that one can see that information has been tampered with, the algorithm is compromised. Payload capacity – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography in other hand requires sufficient embedding capacity.

Robustness against statistical attacks: Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a "signature" when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

Robustness: Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

Independent of file format: With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful existing algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

4. CONCLUSION

For purposes of secret transmission and communication which is prim concern of the proposed concept proposes a concept which has combined effort of two different techniques like cryptography and steganography. Proposed Steganography process is improving image quality and security as compare to the earlier presented technique.

REFERENCES:

[1] 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

[2] R.P Kumar, V. Hemanth, M "Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013, Page(s): 1197 - 1200

[3] 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

[4] 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

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

[6] 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

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

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

[10] AmrM. Riad, Amr H. Hussein and AtefAbou EI-Azm "A New Selective Image Encryption Approach using Hybrid Chaos and Block Cipher "The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Computational Intelligence and Multimedia Computing Track

[11] Arun Raj R, Sudhish N George and Deepthi P. P. "An Expeditious Chaos Based Digital Image Encryption Algorithm" 1st Int'l Conf. on Recent Advances in Information Technology | RAIT-2012 |

[12] Rithmi Mitter and M. Sridevi Sathya Priya "a highly secure cryptosystem for image encryption" IEEE Conferences 2012

[13] Somdip Dey, Kalyan Mondal, Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm" I.J.Modern Education and Computer Science, 2012, 6, 59-67 Published Online June 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijmecs.2012.06.08

[14] S. Premkumar, A.E.Narayanan "Steganography Scheme Using More Surrounding Pixels combined with Visual Cryptography for Secure Application "International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

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

[16] 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

[17] 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

[18] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf and Jules Ehoussou Research on a Normal File Encryption and Decryption" IEEE 2011

[19] Akhil Kaushik, AnantKumar and Manoj Bamela " Block Encryption Standard for Transfer of Data " IEEE International Conference on Networking and Information Technology 2010

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

[21] Danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

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

[23] Ibrahim S I Abuhaiba, Maaly A S Hassan, "Image Encryption Using Differential Evolution Approach" In Frequency Domain Signal & Image Processing : An International Journal (SIPIJ) Vol.2, No.1, March 2011, http://airccse.org/journal/sipij/papers/2111sipij05.pdf

[24] 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.

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

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

[27] 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).

[28] 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)

[29] 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

[30] Jiu-Lun FAN, Xue-Feng ZHANG "Image Encryption Algorithm Based on Chaotic System" Computer-Aided Industrial Design and Conceptual Design, 2006. CAIDCD '06. 7th International Conference on 17-19 Nov. 2006 Page(s):1 - 6

[31] S'ergio, L. C., Salom'ao and Jo'ao M. S. de Alcantara. 2000. Improved IDEA www.cos.ufrj.br/~felipe/ recentpapers/sbcci2000.pd

[32] Anderson, R. J., and F.A.P. Petitcolas. 1998. "On The Limits of Steganography". *IEEE Journal of Selected Areas in Communications*. 16(4): 474-481.

[33] B. Schneier, "Data Guardians," MacWorld, Feb 1993, 145-151.

[34] William stallings, *"Cryptography and Network Security:Principles & Practices"*, second edition.

[35] http://en.wikipedia.org/wiki/ Peak_signal-to-noise_ratio.