IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 5 ISSUE : 2 Print / Issue Publication Date: 12-Aug-2020

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2020.v05i02.086

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 505-507
Published Online June 2020 in IJEAST (http://www.ijeast.com)

AN APPROACH TO PROTECT PARTS OF PROGRAM FROM EXTENSIVE MODIFICATION USING THE CONCEPT OF CRYPTOGRAPHY AND STEGANOGRAPHY

Abhijit D. Shahane
Computer Science & Engineering Department,
P. R. Pote Patil College of Engg. & Management
Amravati, Maharashtra, India

***Abstract*— The major question risen due to rise of internet usage is security and privacy for a data transmission. The continuous work is done by the developers for making use of internet healthy thing, but hackers are a lot intelligent to cope that data. For that purpose, things interacting need to interact in an approach which could not be permitting for listening or for interrupting. Lots of data encryption methods are being used to secure their interacting by many firms. For this work two security methods named, Cryptography and Steganography are being trying. [5-6] By using this methods together, level of information security can be enhanced doubly. The methodology of working of Cryptography and Steganography and their different approaches has been discussed in this paper.**

Keywords— **cipher text, cover image, Encryption, Symmetric Key, Steganography Data Hiding, Cryptography, Decryption.**

I. INTRODUCTION

In the field of computer science, hiding of data is the philosophy of shielding of the blueprint ideas in a computer program that are almost certainly to modify, Hence, shielding another parts of the program from immeasurable mitigation if the blueprint ideas is changed. The shielding contains giving a steady circuitry which covers the remaining of program from the execution. In other words, the capacity to avert explicit features of software element from being available to users, using the programming language methods (like private variables) is called as data hiding.

As soon as confidential message has been inserted, it might get sent across unconfident lines or published in non-private location. Usually, the information rate of secured information imparting using data hiding is lesser in way to keep the secured information unnoticable from the cover channel. This information rate is a bit comparable to the volume of the cover channel. Because of that, digital media is a suitable option for information hiding. [2-5] These days, due to the higher degree of alliance and conspiring in latest information appratus like transpire multimedia sensors, secured transmission become a huge ultimatum for analyzing than never ever. This is crucial to look over methods to recognize and depress secured transmissions such as data hiding in multimedia networkings which gains huge matching up information. [2-5]

The robustness of information shielding gets intensified if it mixes up along cryptography. The phraseology used in information shielding are cover-carrier entity, hidden carrier unit, secret message, and secret key and embedding algorithm. Cover-carrier entity is the transporter of the message like carrier unit, video or audio file. Cover-carrier entity carrying the embedded secret data is the hidden carrier object. Secret message is the information that is to be hidden in a carrier entity. The confidential key is used to implant the message depending on the hiding algorithm [2]. The embedding algorithm is the way, which is used to implant the confidential information in the carrier entity.

The skill as well as science of establishment of cryptosystem that provides data surety is called cryptography. It actually works with the real time securing of digital information. This points to the architecture of procedure based on mathematical algorithms that gives fundamental information safety duties. And it concerns with the architecture of cryptosystems, whereas cryptanalysis is the learning of breakage of cryptosystems. The cryptosystem includes of cipher text, decryption and encryption algorithm, and key, plaintext. The Encryption is plan, which converts plaintext into the Cipher text by the means of Key. The Cipher text is the result got from encryption by applying the encryption key on the plaintext. And Decryption is process of reclaim the plaintext from the cipher text.

A. Symmetric Key Encryption (SKE)

In encryption procedure the identical keys are used for encrypting and decrypting the data which is called as SKE.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 505-507
Published Online June 2020 in IJEAST (http://www.ijeast.com)

Otherwise, in Symmetric key cryptography sender encode the apparent text hold by using secret key and receiver decrypt the cipher text by using the identical key. The normally used algorithms of Symmetric key cryptography are BLOWFISH, DES, 3DES, AES, and many others.

B. Asymmetric Key Encryption (AKE)
In encryption procedure distinctive keys are used for encrypting and decrypting the data which is called as AKE. Otherwise, AK cryptography use one of the two keys i.e. public key and private key that are complementary in method. ECC, RSA, DSA are the example of asymmetric key cryptography.

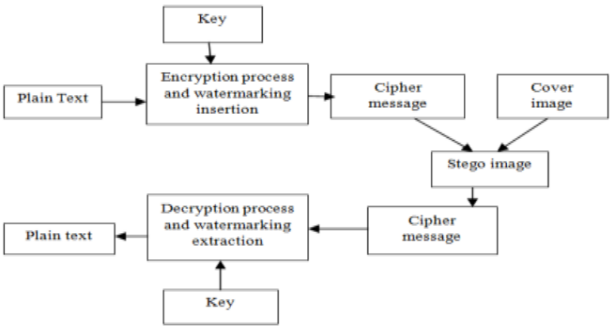
II. LITERATURE REVIEW & RELATED WORK

We have focused on increasing safety and aspect of information hiding. The information hiding uses huge aspiration digital media like a cover signal. It provides the ability to secret a significant quality of information making it different from typical data hiding procedure. Here are the huge burdens like media in media as a cover image. Whole companies need a safe information transmission. At sometime, information hiding cases has incidents in some twist over the cover thing and it can't get back to as it is thing. As opposite to it, in reversible information hiding, the cover thing is losslessly recovered after the message is extracted. The reversible data hiding (RDH) technique is commonly employ in area of law forensics ,medical, and military, here there will be no modification of the original object will be allowed.

The conclusions drawn shows that the shown algorithm maintains the quality of the watermarked picture. The proposed algorithm is also tested using Peak signal-to noise ratio (PSNR).

The advantage of this is that it concludes best PSNR (Peak Signal-to-Noise Ratio) value and computational complexity is minimum. And the disadvantage here is that there is no Key used for information hiding so security level is minimum and easy to hack by hackers.. The additional information is embedded to the image with the use of a data hiding key At the receiver side it will be decrypted. After the decryption it is extracted and the original image will be recovered. If the receiver is not known about the data hiding key he cannot extract the data. So the data will be safe again. When the EOF of the key file occurs, it wraps around. In A-S algorithm has maximum possible substitution which is 256 powers of numbers for the character in the plain text.

III. EXPERIMENT AND RESULT



IV. CONCLUSION

Making it the simple thing, Cryptography and Steganography are the two methodologies used for the purpose of information hiding in the way the secret message can not be developed. The researchers are giving their efforts at this things for enhancing efficiency of the algorithms. This paper discuss about the many researchers gave many algorithms to enhance the information security. In future, this paper will work on the way to enhance the efficiency of algorithms, so the further conclusion may provide a very huge information security.

V. REFERENCE

[1] Ahmed Ch. ," Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[2] Cheng Cheok Yan, "Introduction on Text Compression Using Lempel, Zip, Welch (LZW) method".

[3] Lini Abraham, Neenu Daniel ," Secure Carrier object Encryption Algorithms: A Review", International Journal of Scientific & Technology Research volume 2, issue 4, April 2013, PP-186-189.

[4] Andreas Westfeld and Gritta Wolf," Data hiding in a Media Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.

[5] D. P. Gaikwad and Dr. S.J. Wagh, "Color Image Restoration for Effective Data hiding", i-manager's Journal on Software Engineering, Vol. 4 l No. 3 l January - March 2010 65, pp.65-71.

[6] D.P.Gaikwad and Dr. S.J.Wagh, "Image Restoration Based LSB Data hiding for Color Image", AISA-PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai.

[7] Richard E. Woods & Rafael C. Gonzalez "Digital Image Processing" Book.

[8] X. Zhang, "Reversible data hiding in encrypted carrier objects," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[9] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Carrier objects" Author manuscript, published in "IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".

[10] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas," Data Hiding in Media", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[11] F5 algorithm implementation: 2009, Fridrich, J.R.Du, M. Long: Analysis in Color Images, Binghamton, 2007.

[12] Biswajita Datta, Debnath Bhattacharyya, Samir Kumar Bandyopadhay and Kil-hwan Shin, "High Capacity Signature Hiding Technique in Higher Depth of LSB Layer", Contemporary Engineering Sciences, Vol. 7, 2014, no. 15, 731 – 736.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143