International Journal of Computing Algorithm
Volume: 07, Issue: 01, June 2018, Page No.24-28
ISSN: 2278-2397

A Review on - Data Hiding using Cryptography and Steganography

M. Gajalakshmi[1], R. Vidya[2]
[1]M.Phil Scholar, [2]Assistant Professor
[1,2]PG & Research Department of Computer Science,
St.Joseph's College of Arts and Science, Cuddalore, Tamil Nadu, India.
Email: vidya.sjc@gmail.com, gajalakshmi.mt@gmail.com

Abstract - Security and privacy for a data transmission become a major concern due to rise of internet usage. Many developers are working continuously to make an internet safe environment, but the intruders are very smart to hack the information. For that, two entities communicating need to communicate in a way which is not susceptible to listen in or interception. So every organization uses many data encryption techniques to secure their communication. There are two security mechanisms called, Cryptography and Steganography are being applied. By merging these techniques, two level of information security is achieved. This paper discuss about the way of working Cryptography and Steganography and their different approaches.

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

I. INTRODUCTION

Nowadays sharing commercial and confidential information over the internet is a risky task. As data is transmitted all the way through digital medium has certain demerits like tampering, illegal use, easy to access, copyright violation etc. There are many applications and websites on the internet requires the users to fill their personal data's like telephone number, credit card information, addresses etc. so the users need to communicate with private and secure confidential data transmission over the network. Data integrity and confidentiality are required to protect against unauthorized access and use. Cryptography and steganography are the two common methods play a major role for secure communication. By combining these two methods provides two level security of information sharing. The differentiation between these techniques is computer programs survive that will encrypt a message using cryptography and hide the encryption within an image using steganography. Steganography is combined with cryptography; combination is termed as metamorphic cryptography [18].

Cryptography is the art and science of building a cryptosystem that is able to provide a information security. Cryptography mainly deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. And cryptography concern with the design of cryptosystems, whereas cryptanalysis is the study of breaking the cryptosystems. The cryptosystem contains of plaintext, encryption and decryption algorithm, cipher text and key. The plaintext is the message or data in which normal or readable (not encrypted) form. And Encryption is process, converting plaintext into Cipher text by using Key. The Cipher text is the result from encryption by applying the encryption key on plaintext. And Decryption is process of retrieving the plaintext from the cipher text. Finally Key is the information to control the cryptosystem (cipher system). There are two types of cryptosystems is used, in which encryption-decryption is take place in the system:

i. Symmetric Key Encryption
ii. Asymmetric Key Encryption

A. Symmetric Key Encryption

In encryption process the identical keys are used for encrypting and decrypting the information is called as Symmetric Key Encryption. Otherwise, in Symmetric key cryptography sender encrypts the ostensible text content by using secret key and receiver decrypt the cipher text by using the same key. So there is a requirement

International Journal of Computing Algorithm
Volume: 07, Issue: 01, June 2018, Page No.24-28
ISSN: 2278-2397

to ship the defended key to the receiver along with the cipher text. Secrecy of facts in symmetric key cryptography depends at the confidentiality and length of the secret key. The generally used algorithms of Symmetric key cryptography are DES, 3DES, AES, BLOWFISH and many others [5].

B. Asymmetric Key Encryption

In encryption process distinctive keys are used for encrypting and decrypting the information is called as Asymmetric Key Encryption. Otherwise, asymmetric key cryptography use one of the two keys i.e. public key and private key that are complementary in function. The textual content, that is encrypted the usage of public key, can simplest be decrypted the usage of the subsequent private key. RSA, DSA, ECC are the example of asymmetric key cryptography [5].

Steganography (art of "concealed writing") is used to hide the confidential and sensitive data inside a digital medium. Otherwise, we can called it as hidden communication, i.e., we can hide the secret data (not noticeable by the human eye) into a cover object like image, audio, video, etc. A steganalyst is a person who is skilled in detecting hidden messages from a digital media. Steganalysis is the study of extracting hidden messages from the digital medium which is done with the help of steganography [18].

In Image Steganography it consists of two algorithms, one for *embedding* and another one for *extraction*. The embedding is the procedure of hiding secret message inside a cover media (i.e. cover image), and result of this embedding process is the stego image. The extraction is the process of inversing the embedding process, which reveals the secret message [29].

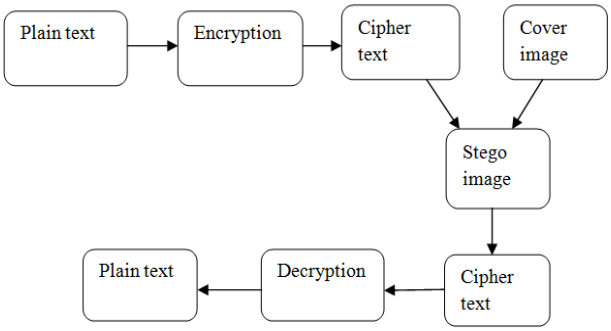

Fig.1. Block Diagram

Different application areas of Steganography are copy right of multimedia object, medical image, military communication, authentication & several areas associated with communication and it has currently reached at a new technology referred to as cloud. Steganography provide the cloud users with data confidentiality, authentication and integrity [1].

So simply it proves that, Cryptography converts the information from its original form (plaintext) into unreadable form (cipher text); where as in steganography, it is the art of hiding messages within other data without changing the data to it attaches, so before and after the process hiding the data almost look like the same. The above figure shows the, Cryptography and Steganography process is carried out in Data hiding technique.

II. RELATED WORK

All the sectors need a secured data transmission. In most instances, data hiding cases has experience in some distortion over the cover object and can't move it back to original cover object. This will be taken place, as some parameter will be distorted over the cover object even after the hidden data has been extracted. But in reversible data hiding, the original cover object is losslessly recovered after the message is extracted [22,23,24,25]. The reversible data hiding (RDH) technique is commonly utilized in area of medical, law forensics and military, here there will be no alteration of the original object will be allowed.

The Reversible Data Hiding technique was first delivered is proposed via Z. Ni et.al. [22], which uses Histogram Shift (HS) approach. An "image histogram" is a type of histogram which illustrates a graphical

International Journal of Computing Algorithm
Volume: 07, Issue: 01, June 2018, Page No.24-28
ISSN: 2278-2397

representation of the pixel value distribution in a digital image. Advantage of this paper is results good PSNR (Peak Signal-to-Noise Ratio) value and computational complexity is low. Disadvantage is of this paper is there is no Key is used for data hiding so security level is low and easy to attack by attackers.

The author X. Zhang [23], overcomes the limitations on Histogram Shifting (HS) and Pixel Value Difference (PVD) methods, here the encryption and decryption process of confidential data and cover image is processed by using data hiding Key. The author W. Hong et.al.[25], overcomes the limitations of previous methods and results by minimizing the error rate. It improves the problems of non-overlapping block method and calculates the smoothness of each block.

The author X. Zhang et.al.[24,26], using image encryption a new feature is added, i.e. if the receiver has only data hiding key means he can able to extract the confidential data, but the receiver does not know the cover image. If the receiver has only encryption key means he can decrypt the cover image cannot extract the confidential data. Advantage of this paper is getting separate privacy for both the confidential data and cover image, medium PSNR value. The author k. Ma et.al.[27], gets the advantage of all the previous approaches and work carried out. The only additional feature is it reserves the space for accommodating the confidential data before the image encryption is carried out. Advantage of this method is high security and good PSNR value. Disadvantage is high computational complexity when comparing other methods [28].

After all this approaches, the extended version of reversible data hiding technique is introduced by the author Achuthshankar et.al.[1]. This method mainly focused on enhancing the image quality by contract enhancement with high security novel lightweight symmetric stream cipher namely A-S algorithm. In this approach introduces the user defined file as a Key instead of generating the Key.

The type of file and size of file will be user defined wish. 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. The user can use the Key file as text file, image, audio, and video. All the privileges are depending upon the user. XOR operation is performed for encrypting the file. Using Histogram Shift method it achieves good and stable PSNR value. Execution time of the algorithm is very low.
It takes the first character of the file plain text file and the first character of the key file and performs an XOR operation which is encrypted as the first character of the cipher text and so on. 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.

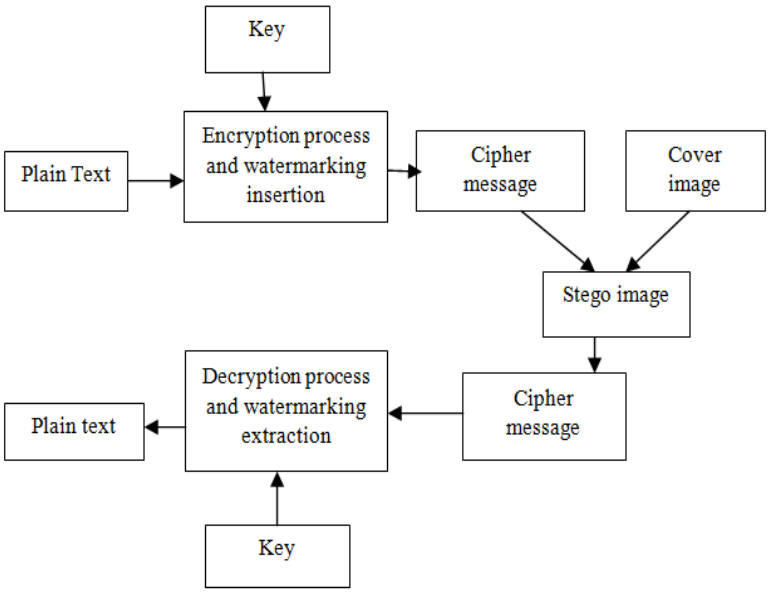

Fig.2. Block Diagram for proposed work

III. RESULT AND DISCUSSION

Execution time of this algorithm when comparing 3DES, IDEA, CAST-128, the A-S algorithm takes 2ms to execute the 50kb file size and 4ms to execute the 250kb file size and vice versa[1]. This approach results in good performance on data hiding. And it is very much safe, simple and faster. The future work of this paper will be minimizing the previous execution time and to deliver the better result in PSNR value with highest security, and also by including Watermarking technique it achieves high security in data transmission. Watermarking is the concept of copyright protection or digital ownership that can read by only authenticated person.

IV. CONCLUSION

In simple words, Cryptography and Steganography is a way to data hiding in such a fashion, presence of hidden message cannot be conceived. Several researchers are working in this area to improve efficiency of the algorithms. In this paper discussed about the various authors proposed a several algorithms and techniques to improve the data security. The future work of this paper will be way to improve the efficiency of the A-S algorithm by using Reversible Data Hiding technique, and including the Watermarking concept, so the result may provide the very high data security.

References

[1] Achuthshankar, A., Achuthshankar, A., Arjun, K. P., & Sreenarayanan, N. M. (2016). Encryption of Reversible Data Hiding for Better Visibility and High Security. Procedia Technology, 25(Raerest), 216–223. https://doi.org/10.1016/j.protcy.2016.08.100

[2] Alam, S. S., & Jianu, R. (2017). Analyzing Eye-Tracking Information in Visualization and Data Space: From Where on the Screen to What on the Screen. IEEE Transactions on Visualization and Computer Graphics, 23(5), 1492–1505. https://doi.org/10.1109/TVCG.2016.2535340

[3] Ansari, N., & Gupta, A. (2017). Image Reconstruction Using Matched Wavelet Estimated from Data Sensed Compressively Using Partial Canonical Identity Matrix. IEEE Transactions on Image Processing, 26(8), 3680–3695. https://doi.org/10.1109/TIP.2017.2700719

[4] Arya, I. G., & Dewangga, P. (2017). A New Approach of Data Hiding in BMP Image Using LSB Steganography and Caesar Vigenere Cipher Cryptography, 12(21), 10626–10636.

[5] Chandra, S., Mandal, B., Alam, S. S., & Bhattacharyya, S. (2015). Content Based Double Encryption

[6] Algorithm Using Symmetric Key Cryptography. Procedia Computer Science, 57(Icrtc), 1228–1234. https://doi.org/10.1016/j.procs.2015.07.420

[7] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010

[8] Dutta, M. K., Singh, A., Soni, K. M., Burget, R., & Riha, K. (2013). Watermarking of digital media with encrypted biometric features for digital ownership. 2013 6th International Conference on Contemporary Computing, IC3 2013, 108–112. https://doi.org/10.1109/IC3.2013.6612172

[9] Gupta, R., & Singh, T. P. (2014). New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters. Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014, 475–479. https://doi.org/10.1109/IC3I.2014.7019643

[10] Hemalatha, S., Acharya, U. D., & Renuka, A. (2014). Wavelet transform based steganography technique to hide audio signals in image. Procedia Computer Science, 47(C), 272–281. https://doi.org/10.1016/j.procs.2015.03.207

[11] Lin, C. C., & Tsai, W. H. (2004). Secret image sharing with steganography and authentication. Journal of Systems and Software, 73(3), 405–414. https://doi.org/10.1016/S0164-1212(03)00239-5

[12] Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017). A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC. IEEE Access, 5(c), 5354–5365. https://doi.org/10.1109/ACCESS.2017.2691581

[13] Nascimento, J. C., & Carneiro, G. (2017). Deep Learning on Sparse Manifolds for Faster Object Segmentation. IEEE Transactions on Image Processing, 26(10), 4978–4990. https://doi.org/10.1109/TIP.2017.2725582

[14] Raypure, R. M., & Keswani, P. V. (2017). Implementation For Data Hiding Using Visual Cryptography. International Research Journal of Engineering and Technology(IRJET), 4(7), 925–928. Retrieved from https://irjet.net/archives/V4/i7/IRJET-V4I7217.pdf

[15] Reddy, M. I. S., & Kumar, A. P. S. (2016). Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm. Procedia Computer Science, 85(Cms), 62–69. https://doi.org/10.1016/j.procs.2016.05.177

[16] Rezghi, M. (2017). A Novel Fast Tensor-Based Preconditioner for Image Restoration. IEEE Transactions on Image Processing, 26(9), 4499–4508. https://doi.org/10.1109/TIP.2017.2716840

[17] Sabnis, S. K., & Awale, R. N. (2016). Statistical Steganalysis of High Capacity Image Steganography with Cryptography. Procedia Computer Science, 79, 321–327. https://doi.org/10.1016/j.procs.2016.03.042

[18] Shivani, Yadav, V. K., & Batham, S. (2015). A Novel Approach of Bulk Data Hiding using Text Steganography. Procedia Computer Science, 57, 1401–1410. https://doi.org/10.1016/j.procs.2015.07.457

[19] Thomas, A. P., Sruthi, P. S., Jacob, J. R., Nair, V. V, & Reeba, R. (2017). Secret Data Transmission Using Combination of Cryptography & Steganography, 4(5), 171–175.

[20] Valandar, M. Y., Ayubi, P., & Barani, M. J. (2017). A new transform domain steganography based on modified logistic chaotic map for color images. Journal of Information Security and Applications, 34, 142–151. https://doi.org/10.1016/j.jisa.2017.04.004

[21] Weng, I. C., & Chen, T. H. (2017). A novel weighted visual cryptography scheme with high visual quality. International Journal of Network Security, 19(6), 922–928. https://doi.org/10.6633/IJNS.201711.19(6).08

[22] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.

[23] X. Zhang, "Reversible Data Hiding With Optimal Value Transfer" IEEE Trans. On Mult., vol. 15, no. 2, pp.316-325, Feb. 2013.

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

[25] W. Hong, T. Chen, and H. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match", IEEE Signal Process. Lett. vol. 19, no. 4, pp.199-202, Apr. 2012.

[26] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[27] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" , IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 533–562, Mar. 2013.

[28] V. Suresh and C. Saraswathy, "Separable Reversible Data Hiding using Compression in Encrypted Image", IJARECE, Vol. 2, Issue 5, May2013.

[29] Saleh, M. E., Aly, A. A., & Omara, F. A. (2016). Data Security Using Cryptography and Steganography Techniques. IJACSA) International Journal of Advanced Computer Science and Applications, 7(6), 390–397.

[30] Vidya, R., Raj, D. V., & Sujatha, K. (2017). Knowledge understanding and advanced searching, 6959(April),1467–1472. https://doi.org/10.21917/ijsc.2017.0203.