Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Hiding Using Cryptography: A Review

Harleen Kaur
Department of computer science & technology
Chandigarh University,
India

Surinder Kaur
Department of computer science & technology
Chandigarh university,
India

Abstract—In this paper we will overview how data hiding can be done using Cryptography. Basically, we will describe how one can use Steganography for hiding data with Cryptography. Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting confidentiality, integrity and availability of information from unauthorized access. In this paper we describe first the data is encrypted using DSA and then MLSB Steganography is applied on it.

Keywords— Steganography, Cryptography, multiple least significant bits (MLSB), Digital signature algorithm (DSA).

I. INTRODUCTION

Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed. Many techniques have been used for hiding the information. Usually the secret information is concealed by the use of cover as not to arouse suspicion if hostile agent discovers the cover.

MLSB Steganography

Multiple least Significant bits steganography is the technique of Steganography in which multiple least significant bits of cover image is replaced by the information to be kept secret. In this randomly bits are selected and replace them with the message bits.

The message is the data that the sender wishes to remain confidential and can be text, audio, video, etc. The *cover* or *host* is the medium in which the message is embedded and serves to hide the presence of the message. It is not required that the cover and the message have homogenous structure. The image with the secretly embedded message produced by encoder is known as *stego-image***.**

Cryptography

It is the art of protecting information by transforming it (*encrypting* it) into an unreadable format called, *cipher text.* Only those who possess a secret key can decipher (*decrypt)* the message into plain text. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and the public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of message uses. Thus using Cryptography alone can only secure the message but for more security purpose Steganography is also applied so that its identity is hidden.

Digital signature algorithm (DSA)

It is a Federal Information Processing Standard for digital signatures. It includes key generation which has two phases. The first choice is choice of algorithm parameters which may be shared between different users of the system, while second phase computes public and private keys for single user .Basically, two steps are involved:

Creation of digital signature: First a hash function is chosen and that hash function is added to the message. This creates a message digest which. Then signature function is added by using private key of the sender. This results in Digital signature as shown in fig.(1).Finally the digital signature so created is transmitted with the plain text i.e. the original information for the receiver.

Verification of digital signature: At the receiving end digital signature is verified. The receiver extracts the message digest by application of signature function and using sender's public key. The receiver the computes the message digest of the retrieved document by applying the same hash function which is used during the creation of digital signature. fig(2).
The authentication and integrity of the document is assumed to be verified if the two message digest so generated match.

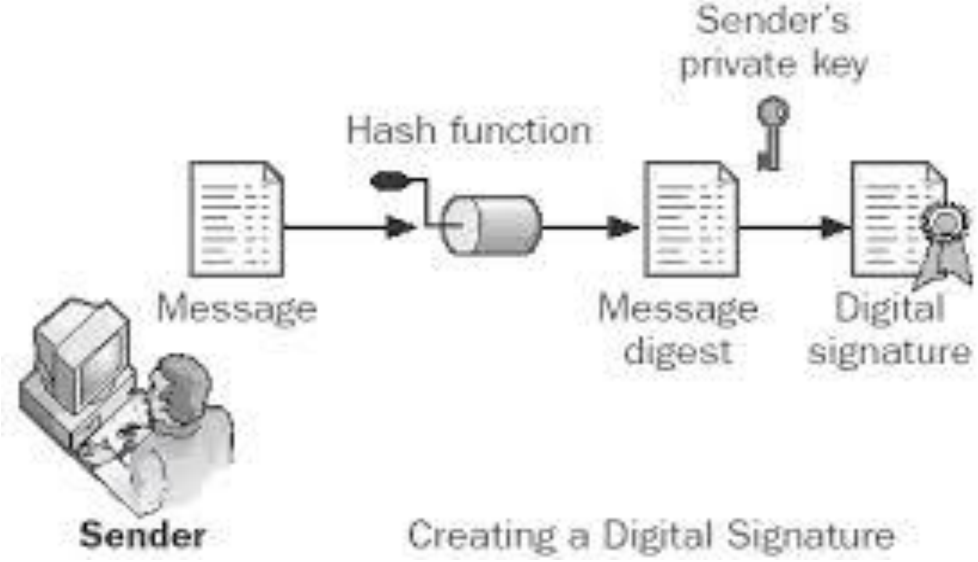

Figure 1 Creating digital signature

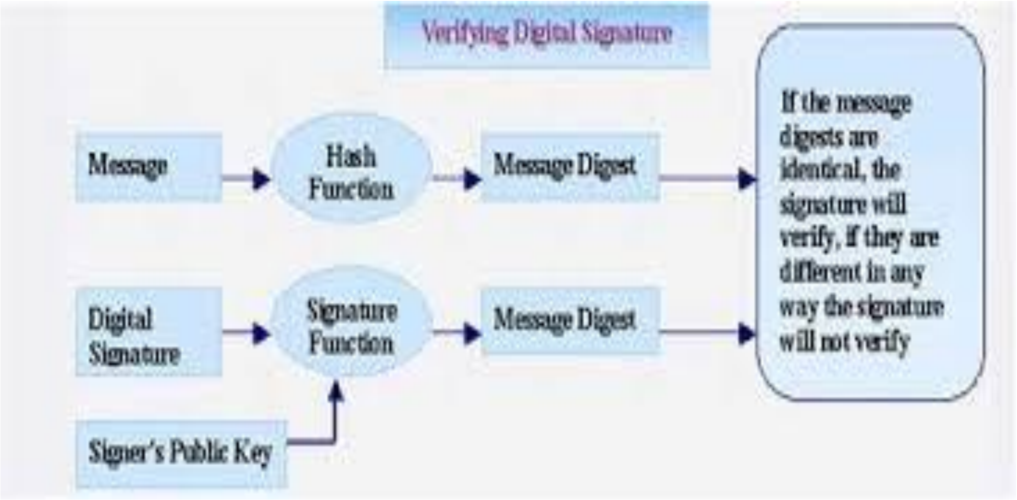
Verifying Digital Signature
Message
Hash Function
Message Digest
Digital Signature
Signature Function
Message Digest
Signer's Public Key
If the message digests are identical, the signature will verify, if they are different in any way the signature will not verify

Figure 2 Verifying digital signature

Benefits of Digital signature:

(a)Confidentiality: It means that encrypted data can only be viewed by intended recipients who have decryption key in hand. Any other interceptor cannot make any sense of it.

(b)Authentication: Encryption can help ensure that data is truly issued by the stated sender and has not been forged by an intruder.

(c)Integrity: It describes the message received so far is not being altered during transmission. It ensures the content of message secure and unaltered.

(d)Non-repudiation: It is most important benefit of using digital signature algorithm. In this case, a sender cannot deny having sent the message.

These all above points are the benefits of digital signature. For more better and secure results cryptography is used with steganography. Otherwise, if alone cryptography alone is used it would have only hide the information. But with the use of cryptography, first the information is being encrypted by applying DSA algorithm and then on this MLSB steganography will be applied which hides it.

Data Hiding technique used: In this paper we have used MLSB steganography for hiding the data. The data required is being encrypted is then hide by using this steganography technique. So far LSB embedding is used in which the bits of message is directly embedded into the least significant bits of the cover image in a deterministic sequence. Modulating the least-significant bits does not result in human-perceptible difference because the amplitude of the change is small. However there are many weakness when robustness, tamper resistance, and other security issues are considered. MLSB steganography is classified into two categories:

1) TMLSB Steganography: Randomly select samples and replace their *l* LSBs with the message fragments with size of *l.* This category is called TMLSB steganography("T" is the shortening of" typical"), such as T2LSB steganography for *l* = 2.

2) IMLSB Steganography: Randomly select bits from the *l* LSBs planes and replace them with message bits. This category is called as IMLSB steganography ("I" signifies the independence of the effects on different bit planes), such as I2LSB steganography *l* = 2.

After various quantitative steganalysis methods applied on these above MLSB steganography methods. It is obtained that IMLSB is more efficient then the TMLSB.

II. PROPOSED WORK

No Neither Cryptography or Steganography can alone make the data secure efficiently. So a better technique is developed by combining two techniques. A combination of steganography and cryptography is used which take the advantage of both the techniques. We are using Digital Signature Algorithm for encrypting the message the message to be hidden inside an image to make it unreadable and secure. After encryption we will apply MLSB steganography for further enhancing the security. In the previous sections we have already described how these two techniques work and what are the benefit of using the DSA and MLSB steganography.

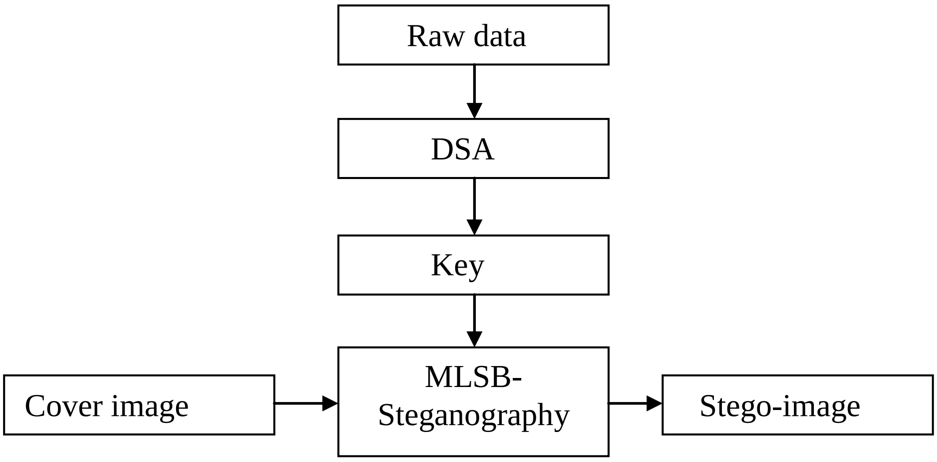

Figure 3. Steps of data security and data hiding

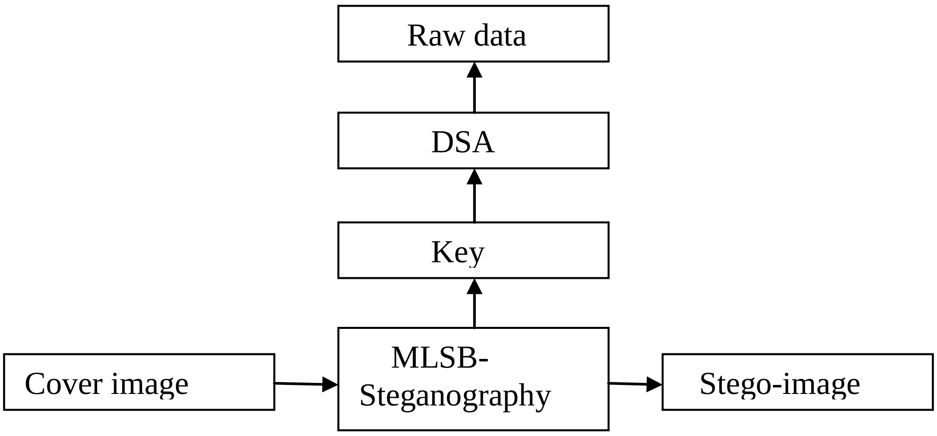

Figure 4. Obtaining the raw data from the Stego- image

by the sender. And in this way the receiver obtain the secret message to be read.

III. FUTURE WORK

When the above method is applied to hide a data using cryptography. Ten a secure image is formed. But not only here the works stops. The next step is to obtain the parameters i.e. PSNR, MSE and compare them. On the other hand MLSB and cryptography is a new technique and we expect the results of hiding to be far better in comparison to the previous technique. merge amount of different kind of data is communicated over the network. Energy efficiency is the most required quality in a sensor network where each node consumes some energy with each transmission over the network. Energy efficiency is required to improve the network life. The existing work is defined in the same direction to improve the network life but still there is need to improve the efficiency of the sensor network. The purpose of the work is to enhance the security for data hiding and to compare the values of high capacity blind steganography techniques with the new implemented techniques.

IV. CONCLUSION

In this paper two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. DSA is used in this paper which is better then RSA in the fact that it is more fast at generating keys, fast at decrypting. MLSB is used as a steganographic technique for the fact that previously when LSB embedding is used it created so many problems i.e. Moreover, this can method i.e. data hiding using cryptography can be used in many future works. Its results helps us to compare the results with many parameters i.e. PSNR, MSE, etc.

ACKNOWLEDGEMENT

Author would like to give her sincere gratitude to guide Ms. Surinder Kaur who encouraged and guided her throughout this paper.

REFERNCES

[1] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantative Steganaylsis for Multiple Least Significant Bits Steganography", *IEEE Transaction on Information Forensics and Security, Vol. 8, No.1,* January 2013.

[2] Parah, A, Shabir., Sheikh, A, Javaid., and Bhat,G.M., 2012. "Data Hiding In intermediate Significant Planes, A High Capacity Blind Steganographic Technique" 2012- *International Conference on Emerging Trends in Science, Engineering and Technology*.

[3] Singh , Ajit., Malik Swati., 2013. "Securing Data by using Cryptography With Steganography". Universal *Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 5, May 2013.

[4] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," *IEEE Multimedia, Special Issue on Security*,
vol. 8, no. 4, pp. 22–28, Oct./Dec. 2001.

[5] S. Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7,pp. 1995–2007, Jul. 2003.

[6] J. Fridrich and M. Goljan, "On estimation of secret message lengthbin LSB steganography in spatial domain," in *Proc. SPIE, Security,Steganography, and Watermarking of Multimedia Contents VI*, E. J.Delp, III and P. W. Wong, Eds., San Jose, CA, 2004, vol. 5306, pp.
23–34.

[7] Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. *IEEE Computer Society*. IEEE Security and Privacy, pp. 32-44.

[8] Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. *International Journal of Computer Technology Application*, 2(3), ISSN: 2229-6093, pp. 626-630

[9] A. Ker, "A general framework for the structural steganalysis of LSB replacement," in *Proc. 7th Information Hiding Workshop, LNCS*, B.Mauro, H. J. Jordi, K. Stefan, and P. G. Fernando, Eds., Barcelona ,Spain, 2005, vol. 3727, pp. 296–311.

[10] S. Dumitrescu and X. Wu, "A new framework of LSB steganalysis of digital media," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp.3936–3947, Oct. 2005.

[11] X. Yu, T. Tan, and Y. Wang, "Extended optimization method of LSB steganalysis," in *Proc. IEEE Int. Conf. Image Processing*, Genoa, Italy,2005, vol. 2, pp. 1102–1105.

[12] X. Yu and N. Babaguchi, "Weighted stego-image based steganalysis in multiple least significant bits," in *Proc. IEEE Int. Conf. Multimedia &Expo*, Hannover, Germany, 2008, pp. 265–268.

[13 A. Ker, "Steganalysis of embedding in two least-significant bits," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 46–54, Mar. 2007.

[14] X. Luo, C. Yang, D. Wang, and F. Liu, "LTSB steganalysis based on quartic equation," *LNCS Trans. Data Hiding Multimedia Security II*,vol. 4499, pp. 68–90, 2007.

[15] C. Yang, F. Liu, X. Luo, and B. Liu, "Steganalysis frameworks of embeddingin multiple least-significant bits," *IEEE Trans. Inf. ForensicsSecurity*, vol. 3, no. 4, pp. 662–672, Dec. 2008.

[16] T. Pevný, J. Fridrich, and A. Ker, "From blind to quantitative steganalysis,"*IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 445–454,
Apr. 2012.

[17] A. Ker, "Fourth-order structural steganalysis and analysis of coverassumptions," in *Proc. SPIE, Security, Steganography, and Watermarkingof Multimedia Contents VIII*, E. J. Delp, III and P.W.Wong,Eds., San Jose, CA, 2006, vol. 6072, pp. 25–38.

[18] J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, "Quantitative steganalysis of digital images: Estimating the secret message length,"*ACM Multimedia Syst. J., Special Issue on Multimedia Security*, vol.9, no. 3, pp. 288–302, 2003.

[19] A. Ker, "Derivation of error distribution in least squares steganalysis,"*IEEE Trans. Inf. Forensics Security*, vol. 2, no. 2, pp. 140–148, Jun.2007.