Secure Data Hiding using Cryptography And LSB Techniques

Shambhavi U. Burge, Nitin A. Sawant ,Swapnil D. Choudhari, Priyanka A. Sonkusare

Abstract— Steganography means, a method for hiding secret information for example password text or image inside a cover file. In this paper, a combination of audio steganography and image steganography is used and also forensic tec. The aim is to hide secret data in the audio and image of a video file. Video has so many still frames of image and audio, we can select any frame for hiding our data. Two algorithms can be used for this purpose.4LSB for image steganography and phase coding algorithm for audio steganography.
.

Index Terms—4LSB, Data Hiding, Steganography, Computer Forensics, Histogram, PSNR, Authentication.

I. INTRODUCTION

With the rapid development of digital technology and communication media, data such as text, images, audio, video, etc. are growing importance in day to day life. A large amount of data is being transmitted over internet. There is always a threat of an intruder accessing the private information. So a mechanism needs to be implemented in order to keep the integrity and confidentiality of the information. This has led to an explosive growth in the field of information hiding.

Cryptography is the most common word that is used in information hiding. Cryptography means converting the text from readable format to unreadable format. Cryptography applies encryption techniques to convert the message into non-readable form but it does not hides the message i.e., the encrypted message is visible [1]. It would be great to have something that can embed the secret message into some media in such a way that no one can guess whether anything is hidden or not.

are continually searching for new methods for steganography [3]

Shambhavi U. Burge,*Computer Department, Pune University Pune,,Mobile-9689416664*
Nitin A. Sawant Computer Department, Pune University Pune,,Mobile-9096094028
Swapnil D. Choudhari Computer Department, Pune University Pune,,Mobile-9923097316
Priyanka A. Sonkusare Computer Department, Pune University Pune,,Mobile-8446899077

II. APPLICATIONS OF STEGANOGRAPHY

Steganography can be used for wide range of applications such as, in defense organizations for safe circulation of secret data, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials [5]. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost[1], in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviours[2], for data hiding in countries where cryptography is prohibited, in improving mobile banking security[3], in tamper proofing so as to prevent or detect unauthorized modifications and other numerous applications [10]

III. RELATED WORK

The paper discusses the combination of cryptography with adaptive steganography for audio video sequence with LSB as the encryption algorithm.as the encryption increases the PSNR value also gets increased.[05]The author discusses different methods for audio steganography and LSB method is found to be more secure.[02]The paper discusses LSB audio steganography with location identification and it provides good audio quality and robustness. [06]The paper discusses the different audio steganography methods such as echo hiding, parity hiding, phase coding and their comparison. [07]The author explains how an image can be hidden in AVI video using 4LSB method. Security techniques are used to find the parameters such as frame number, height and width of the image, PSNR and histogram of the image before and after hiding. If all the verification of these parameters are found to be correct the data is send to receiver. Fig 1 shows the block diagram of the proposed method

IV. EXISTING SYSTEM

1) Cryptography And Hashing System

Cryptography technique can convert the plain text to encrypted text. The encrypted information can decrypt the intruder by get the key information. A single key is used for both contrast to Cryptography, where the enemy is allowed to encryption and decryption. The sender uses the key (or detect, intercept and modify messages without being able some set of rules) to encrypt the plaintext and sends them to violate certain security premises guaranteed by a cipher text to the receiver [15] . The receiver applies the same cryptosystem, the goal of Steganography is to hide key (or rule set) to decrypt the message and recover the messages inside other harmless messages in a way that plaintext [15].

3868

Advantages :-
1. In cryptography we easily hide the information using symmetric and asymmetric key .
2. Cryptography is most useful to secure data hiding or transmission.
    Disadvantages:-
1. Using cryptography system large scale data cannot be transfer.
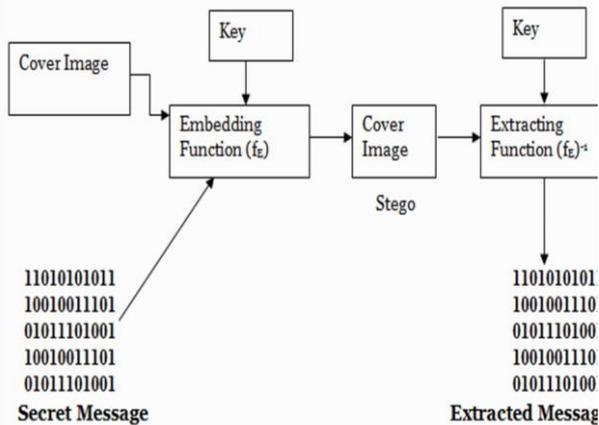2. This system doesn't provide more security.

Fig1. Cryptography And Hashing System

2) Image processing system using Median filter

A median filter is a non-linear digital filter which is able to preserve sharp signal changes and is very effective in removing impulse noise (or salt and pepper noise) [14]. An impulse noise has a gray level with her or lower value that is different from the neighborhood point. Linear filters have no ability to remove this type of noise without affecting the distinguishing characteristics of the signal. Median filters have remarkable advantages over linear filters for this particular type of noise. A standard median operation is implemented by sliding a window of odd size (e.g. 3x3 window) over an image. At each window position the sampled values of signal or image are sorted, and the median value of the samples replaces the sample in the center of the window as shown in Figure 2.
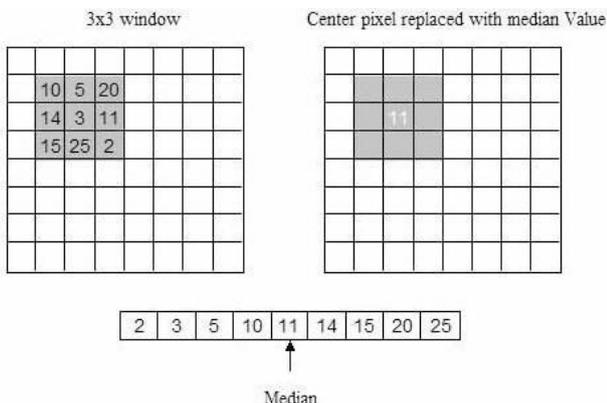

Fig2. Image processing system

Advantages
1. Median filters have remarkable advantages over linear filters for this particular type of noise. Therefore median

filter is very widely used in digital signal and image/video processing applications.

Disadvantages
1. Image processing system can not transfer lager data .

3) LSB Technique

In LSB technique to hide the data behind the image we uses 1LSB.Most of the steganography applications hide data inside images using variation of least significant bit (LSB) embedding technique [13]. LSB embedding data is hidden in the least significant bit of each byte in the image. By using stego analysis techniques data hidden inside an image using normal LSB technique.But not only it hides the user's data (secret image) within an image, but it also compresses & encrypts the user's data [13] Least significant bit insertion is one of the most common and technical embedding technique for hiding data inside the cover file. The amount of data to be hidden inside the image depends upon the size of the image and the number of least significant bits to be used. LSB insertion works simply just by replacing least significant bit of every pixel in cover image with the data to be hidden. For example letter a (10000011) can be hidden using LSB insertion [13].

Pixel values before LSB insertion:
        11000000 01001110 11110011
        00000011 10101011 11000101
        10000110 11111100 11000000

Pixel values after LSB insertion of 'A' will be:
        11000001 01001110 11110010
        00000010 10101010 11000100
        10000110 11111101 11000001

Altering the least significant bits will result in a color slightly different from the original one which is unable to be detected by human eye. The reason being human eye is not sensitive enough to recognize the difference in color between pixels which differs by just 1 unit.

Advantages
1. Using LSB techniques providing strong encrypting key to secure data .
2. Encryptions of the message, so that who extracts it must also decrypt it before it make sense.

V.   Conclusion

We conclude that, from three systems which we studied, namely, cryptography and hashing system[15], image processing and filtering system[16], LSB system[14].We found some drawback. In cryptography and hashing system its not highly secured. In image processing and filtering system PSNR value is less. In LSB system it does not provide good security. Hence we use Antiforensics technique because it provides high security, has high PSNR value and data recovery is accurate.

VI.   References

[1]   N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography", *IEEE Conference on Security and Privacy*, pp. 32-44, 2003.
[2]   Pathak.P, A.K.; Nag.A"A New Audio Steganography Scheme based on Location Selection with Enhanced Security", ACES First International Conference 2014.

[3] Rajput A.S., Mishra N., and Sharma S., "Towards the growth of image Encryption and Authentication Schemes", *International Conference on Advances in Computing, Communications and Informatics* (ICACCI), 2013.

[4] BassemBakhache, Joseph M. Ghazal, and Safwan El Assad,"Improvement of the Security of ZigBee by a New Chaotic Algorithm", IEEE Systems Journal 2013.

[5] V.Sathyal, K.Balasuhramaniyam, N.Murali, M.Rajakumaran, Vigneswari,"data hiding in audio signal, video signaltext and jpeg images",IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012)

[6] "Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm".Praveen. P[1], Arun. R[2]*M.Tech, Asst. Prof, Dept of Computer Science and Engineering, Shree NarayanaGurukulam College of Engineering, Kadayiruppu, Ernakulam, Kerala* .

[7] K.A Navas, Vidya.V, Sonia.V.Dass,"High security data embedding in video",Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE.

[8] FatihaDjebbar, BeghdadAyad, HabibHamamandKarim Abed-Meraim,"A view on latest audio steganography techniques", International Conference on innovations in Information Technology 2011.

[9] MohMohZan and Nyein Aye, "A Modified High Capacity Image Steganography using Discrete Wavelet Transform", *International Journal of Engineering Research & Technology* (IJERT), Vol. 2, August 2013.

[10] Jessica Fridrich and Jan Kodovsky, "Rich Models for Steganalysis of Digital Images",IEEE *Transactions on Information Forensics and Security,* Vol. 7, No. 3, pp. 868-882, June 2012.

[11] Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang, "VQ Applications in Steganographic Data Hiding Upon Multimedia Images", *IEEE Systems Journal*, Vol. 5, No. 4, pp. 528-537, December 2011.

[12] A S. Radharani Dr. M.L. Valarmathi, Ph.D. "Study on Watermarking Schemes for Image Authentication "International Journal of Computer Applications (0975 – 8887), Volume 2 – No.4, June 2010.

[13] D. Sandipan, A. Ajith, and S. Sugata," An LSB Data Hiding Technique using Prime Numbers", *Third International Symposium on Information Assurance and Security, Manchester, UK, IEEE CS press*, 2007.

[14] Roy, S. (2014), "Online payment system using steganography and visual cryptography", Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE

[15] Arup kumarBhaumik, Minkyachoi, "Data hiding in video" IEEE International journal of da ta base a application,vol.2no.2june2009. pp.9-15

[16] Cheng, Z.; Kim, Se-Min &Yoo, Kee-Young. A new direction method by modulus operation. *Int. J. Signal* steganography scheme based on an index-colour image. *Proc., Image Proc. Pattern*, 2009, **2**(1), 79-88.*In* the 6th International Conference on Information 23. Shamir, A. How to share a secret. *Communication of the* Technology: New Generations,

las Vegas, Nevada, 2009, *ACM*, 1979, **22**, 612-13. pp. 376-81.

Shambhavi U. Burge, *Computer Department, Pune University Pune,,Mobile-9689416664*

Nitin A. Sawant Computer Department, Pune University Pune,,Mobile-9096094028

Swapnil D. Choudhari Computer Department, Pune University Pune,,Mobile-9923097316

Priyanka A. Sonkusare Computer Department, Pune University Pune,,Mobile-8446899077

.