International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.4, pg :134-138 01 Oct. 2012

DUAL LAYER DATA HIDING USING CRYPTOGRAPHY AND STEGANOGRAPHY

Dipesh G. Kamdar[1], Dolly Patira[2], Dr. C. H. Vithalani[3]

[1]Department of Electronics and Communication, JJ Tibrewala University, Jhunjhunu, Rajasthan, India - 333001
[2]Department of Computer Engineering, VVP Engineering College, Rajkot, Gujarat, India - 360005
[3]Department of Electronics and Communication, Government Engineering College, Rajkot,Gujarat, India - 360005
kamdardipesh@gmail.com, dollypatira@gmail.com, c_h_vithalani@yahoo.com

ABSTRACT: Digital communication has become an essential part of society. Nowadays, a lot of applications are internet based and it is important that communication be made faithful and secret. Steganography and Cryptography are two popular ways of information exchange in a secret way. Steganography hides the existence of the message and the Cryptography distorts the message itself. Using Cryptography, the data is transformed into some other garbage form and then the encrypted data is transmitted. In steganography, data is embedded in a digital file (cover, normally image or video) and the digital file is transmitted. If secrete message converted to cryptography it will result in garbage form and always comes under suspect to be have a hidden data. If secrete message is hide in other digital cover using steganography, then it might be identified by steganalysis tools. In either ways, weather cryptography or steganography is used, though it is always chance that hidden message is getting detected. In order to make faithful and secure communication, a dual layer hiding technique is proposed in this paper.

KEYWORDS—Steganography, Cryptography, DCT, Public Key, Private Key

I. Introduction

Steganography is an art of hiding the information inside the cover information in such a way that it appears as normal cover though it contains the hidden information [1]. Traditionally Image and Video files are used as cover for digital Steganography; and hence lots of Steganalysis tools are developed [2] too. Steganalysis tools watch out the cover image or video for frequency domain, least significant bit replacement, DCT based Steganography, and detect the presence of the hidden information [3]. If hidden information is found, it needs to be extracted out manually for meaningful information. Here, proposed system is for hiding the text or image in dual layer over video using Cryptography and Steganography. The information is first hide inside small size of the image file using encryption algorithm using public key [4], results in the garbage image. The generated garbage image is again hiding inside video file using random replacement of data in DCT domain selected based on private key. The stego-video may have larger size, but it is not possible for any steganalysis tools to find hidden information inside the stego-video, as it is protected with dual layer random allocation of DCT with private key and encryption algorithm using Public Key. The MATLAB based script is used to generate result.

II. Cryptography

The information which needs to share secretly can be send via cryptography. The cryptography results in ciphered information [5], which looks like a garbage, and always looks doubtful for having hidden information inside it. The simplest algorithm is shown in the figure 1(a), which is used here for cryptography. The Encryption Key Generator generates the Encryption Key and Public Key [6], using which Information is gets encrypted by encryptor. The Encrypted Information is then sending to receiving end.

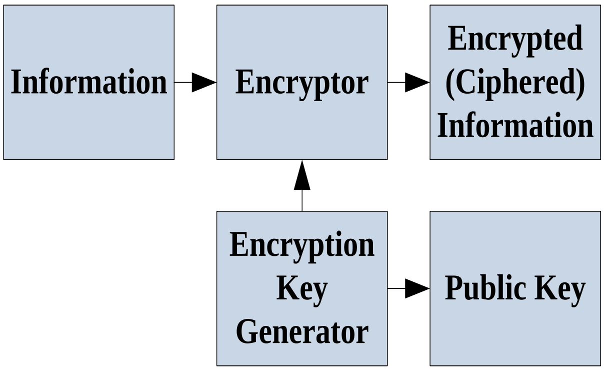
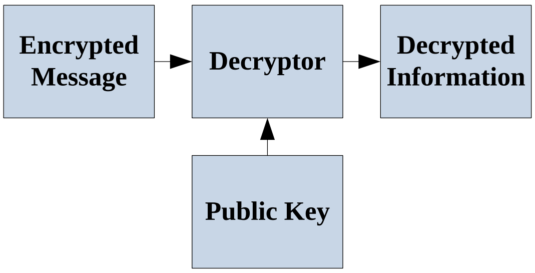


Fig. 1 (a) – Simplified Cryptography Encryptor



1 (b) – Simplified Cryptography Decryptor

The simplified cryptography decryptor is shown in the figure 1 (b). The cryptography decryptor retrieves original information with the help of public key.

III. Steganography

Steganography is an art of hiding the information inside the cover in such a way that, it looks like simple cover, though it has hidden information [1]. Simplified Proposed Steganography system is shown in the figure 2 (a).

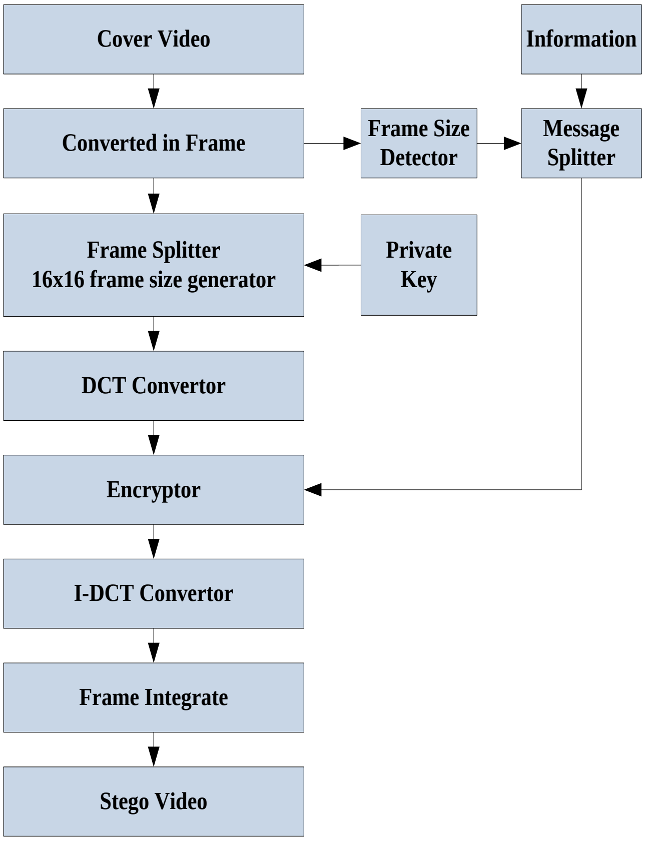


Fig. 2 (a) – Steganography Encryptor

Frames are extracted out of the small size cover video file. The information is splited in some small portion depends on the size of the frame of cover video. From, each frame, small 16*16 pixel group is selected depends on private key. This makes the selected groups look likes random, to those who don't have private key. The selected pixel group is then converted in to frequency domain using discrete cosine transform (DCT) [7]. Predefine portion of the frequency domain data is replaced by the spilled message portion, and reconverted to spatial domain using Inverse DCT, and put back on to the frame. The process continues till full message in encrypted into the frames. The frames are integrated to create stego-video as shown in figure 2 (a).

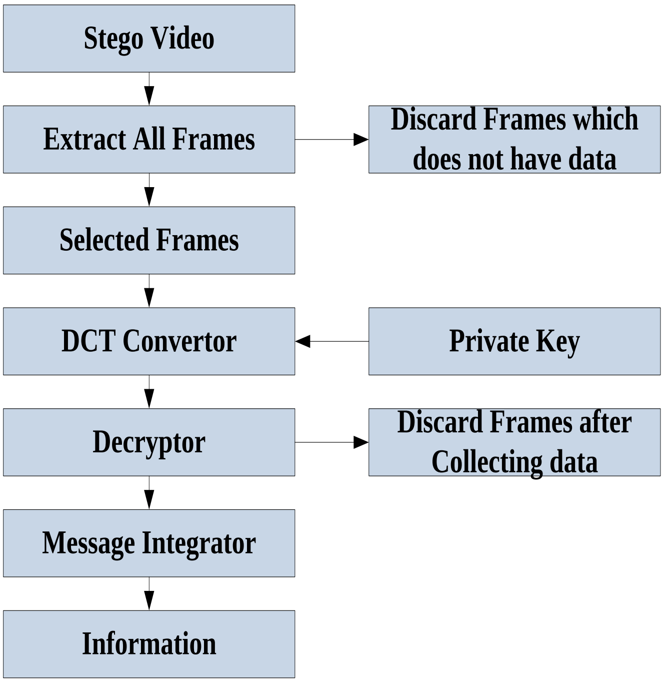


Fig. 2 (b) – Steganography Decryptor

Steganography Encoder, need to put some information in the video for the receiver, by which receiver can understand the data format, way of hiding, kind of encryption, etc. This is call rule list for steganography, which is generated and also placed over the first frame of video file, as a reference for receiver.
Steganography Decryptor is shown in figure 2(b). It is easy to understand form the figure that, if the Private Key is not known, it is not possible to find the hidden message. Though, if Brute Force method is used, or any other steganalysis tools are utilized, there is a bit chance that, on bad day, the hidden message can get detected.

IV. Dual Layer Cryptography and Steganography

The proposed algorithm is to combine the cryptography and steganography [8] to hide the information. Information is made garbage using cryptography, and then stored in cover video using steganography. Hence, even by using the any Brute Force methods or steganalysis tools are not able to find the hidden information.

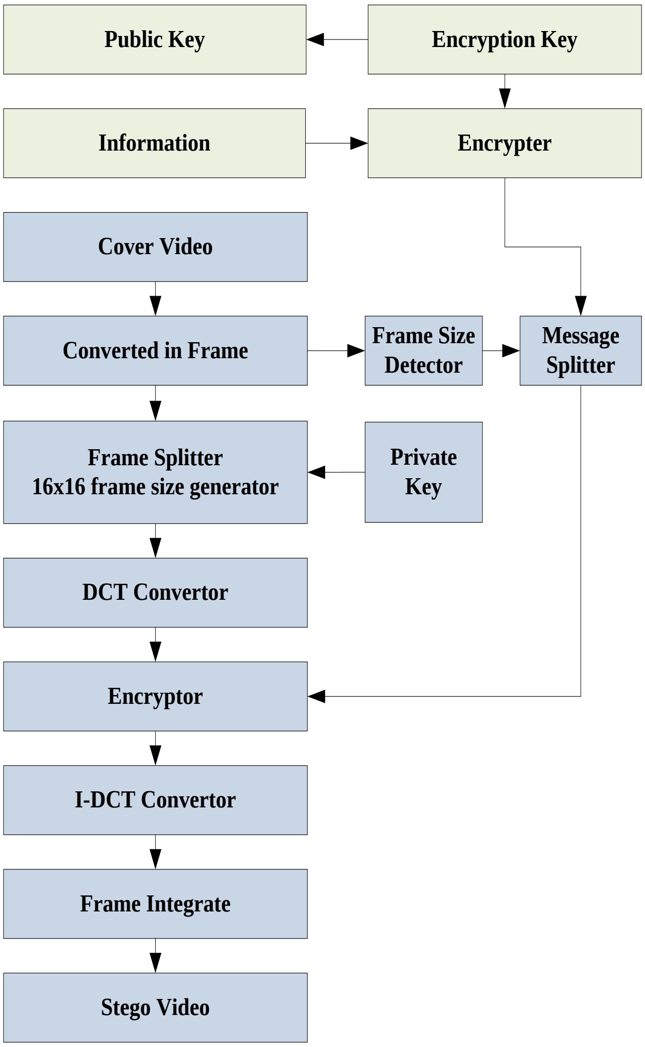


Fig. 3(a) – Dual Layer Embedding for data hiding

As using any technique for steganography detection, as message that hidden is encrypted (i.e. message is in the garbage form), everything is looks garbage and from this it is not possible to find out that which garbage is message and which is really garbage data. The proposed system has video as the cover, and hence do not put any restriction over the information to be hide like happened over the image steganography. The results are in terms of the video file and hence cannot be printed over paper.

The Dual Layer Steganography and Cryptography detector is shown in the figure 3(b). The decryption algorithm depends on the prior knowledge of private key and public key. If both public and private key are known to the receiver, the original message can be regenerated. The receiver also gets information about the data type, way of hiding, kind of encryption used, etc from the first frame of video file, and can able to retrieve the original information from the prior knowledge of private and public key only.

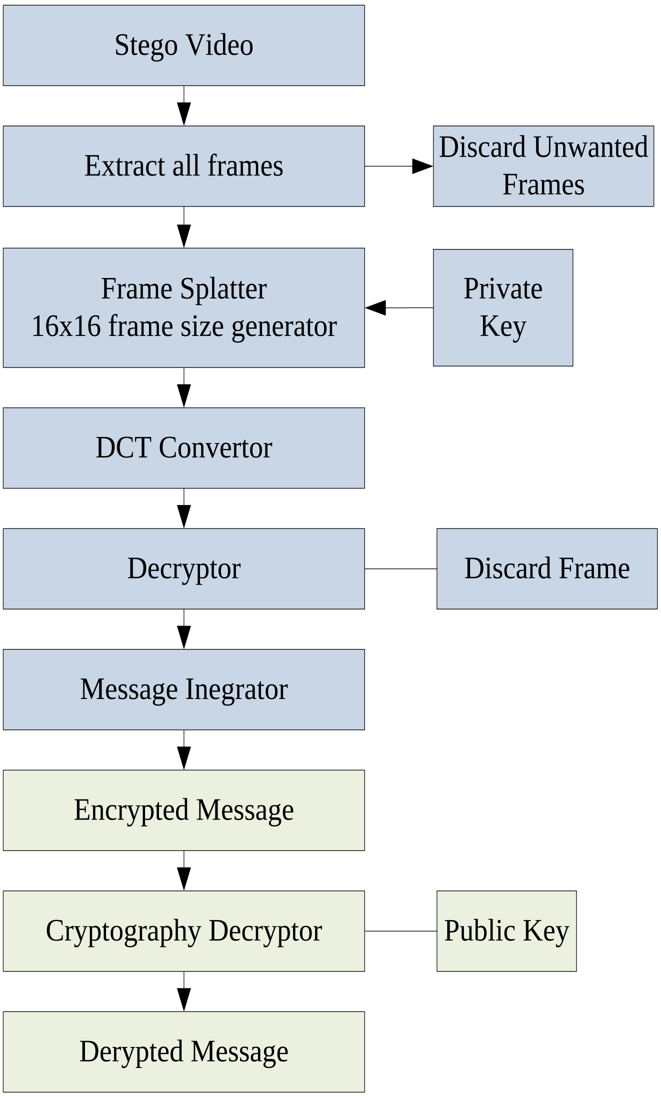
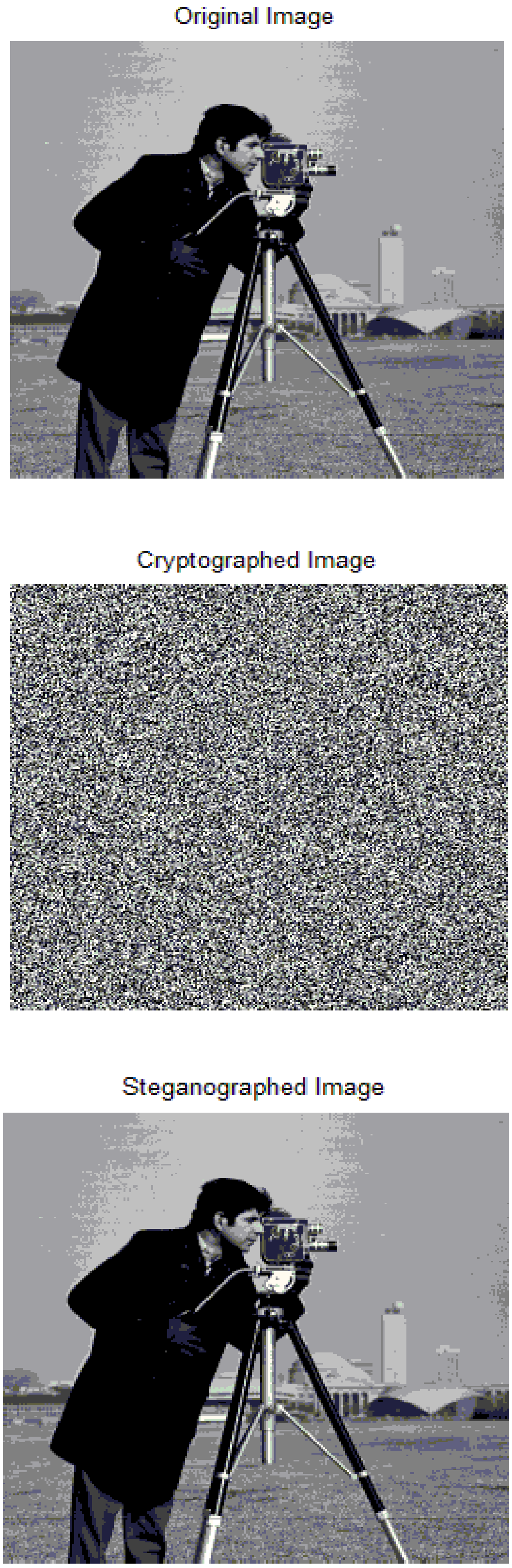


Fig 3 (b) – Dual Layer Decryptor for data retrieval

V. RESULTS AND DISCUSSION

The result is in terms of video and cannot be shown here on the page. The intermediate results are in terms of image and are shown in the figure 4.

The original image is shown in figure 4(a). The resulting of image cryptography using public key is shown in figure 4(b). The resulting image of Steganography using discrete cosine transform (DCT) is shown in figure 4(c). It can be easily seen in the cryptography image results in the garbage image, while Steganography results in the image that looks like original image. If steganographed image is tried to hide inside video, it can be found by the steganalysis tools. If cryptography based image is used, any steganalysis tools cannot find the hidden data as it is garbage. The final result comes in terms of video, hence not shown over the paper.



Original Image

Cryptographed Image

Steganographed Image

Fig. 4 – (a) Original (b) Cryptographic (c) Steganography Image

VI. Conclusion

The single layer Cryptography always results in the suspected object, while steganography can be detected by the steganalysis tools. Dual layer steganography, can also be get detected by some of the new steganalysis tools. Hence, these cannot be considered as the surely secured method for secrete information sharing. The combination of the cryptography and steganography i.e. crypto-steganography [9] along with the presence of public key and private key, it becomes safest way for passing secure information over any communication channel.

VII. References

[1] Changder, S.; Ghosh, D.; Debnath, N.C.; , "Linguistic approach for text steganography through Indian text," Computer Technology and Development (ICCTD), 2010 2nd International Conference on , vol., no., pp.318-322, 2-4 Nov. 2010

[2] Budhia, U.; Kundur, D.; Zourntos, T.; , "Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain," Information Forensics and Security, IEEE Transactions on , vol.1, no.4, pp.502-516, Dec. 2006

[3] Manikopoulos, C.; Yun-Qing Shi; Sui Song; Zheng Zhang; Zhicheng Ni; Dekun Zou; , "Detection of block DCT-based steganography in gray-scale images," Multimedia Signal Processing, 2002 IEEE Workshop on , vol., no., pp. 355- 358, 9-11 Dec. 2002

[4] Dhakar, R.S.; Gupta, A.K.; Sharma, P.; , "Modified RSA Encryption Algorithm (MREA)," Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on , vol., no., pp.426-429, 7-8 Jan. 2012

[5] Joshi, A.; Joshi, B.; , "A randomized approach for cryptography," Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on , vol., no., pp.293-296, 22-24 April 2011

[6] Siad, A.; , "Anonymous Identity-Based Encryption with Distributed Private-Key Generator and Searchable Encryption," New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on , vol., no., pp.1-8, 7-10 May 2012

[7] Raftari, Neda; Moghadam, Amir Masoud Eftekhari; , "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT," Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on , vol., no., pp.295-300, 24-26 July 2012

[8] Yi-Hui Chen, Chiao-Chih Huang, Chi-Shiang Chan; , "Double Layer Data Embedding Scheme Based on Three-Pixel Difference" Journal of Electronics Science and Technology, Vol. 9, No. 4, December 2011.

[9] Abhishek Patidar, Gajendra Jagnade, Laxmi Madhuri, Pranay Mehta, Ronak Sheth; "Data Security using crypto-steganography in web application", Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol 3, No.4, 2012.