Evaluation Performance of Cryptography-Stenography using PSNR and BCR Result

Ms. K.V.Kalaria
Lecturer
Information Technology Department
Government Polytechnic,Rajkot,Gujarat,India.

Abstract— In recent past few years, information sharing and transfer has increased exponentially using Digital Communication, internet technology, and while sharing data, it is important that communication must be faithful and secure. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. Cryptography and Steganography are two popular ways of information exchange in a secret way, where Steganography hides the existence of the message and the Cryptography distorts the message itself. In Cryptography techniques, the data is encrypted and results into some useless form and then the encrypted data is transmitted, which always comes under the suspect to be have a secrete message. In steganography techniques, data is embedded in a cover file (normally digital image or video) and the digital file is transmitted. If the digital file is tested with steganalysis tools, then secrete data may be easily explored. In either ways, weather cryptography or steganography is used, though it is always chance that hidden message is getting detected. In order to improve the security, fusion of cryptography and steganography is used, known as cryptography-steganography. In this paper, important parameters are measured and comparative analysis is computed for various cryptography techniques used for crypto-steganography.

Key words: Cryptography, Steganography, Cryptography-Steganography.

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 verify the cover image or video in various different ways, like frequency domain, LSB (Least Significant Bit) replacement, DCT (Discrete Cosine Transform) domain, and detect the presence of the hidden information [3]. If hidden information is found, it may be extracted out.

Cryptography is used to convert information into encrypted form in such a way that it becomes garbage, and only intended receivers are able to recover the data from that useless data. Though, some unintended receivers, uses the cryptanalysis tools may able to recover the information.

As steganography and cryptography are well known and famous techniques, steganalysis and cryptanalysis tools are developed too. The fusion of this two techniques, namely crypto-steganography, takes the advantages of both techniques, while eliminates the limitations of these techniques, is used in this paper.

Here, different cryptography techniques are used over same data to generate different results, and these encrypted data is made hide inside the cover video using LSB replacement based Steganography techniques, to compute various performance parameters of resultants crypto-stego video.

II. Cryptography

Cryptography can be used to share the information secretly. The cryptography results in cipher information called garbage [5] and always look doubtful as 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 used to generate the Encryption Key and Public Key [6], using which Information is encrypted. Then that encrypted information is send to receiving end.

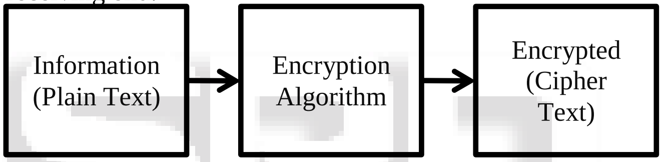


Fig. 2 (a): Simplified Cryptography Encryption

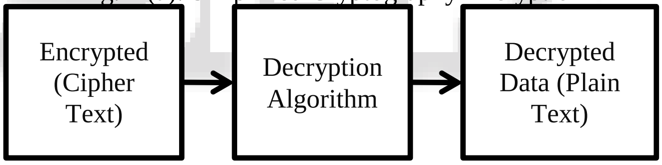


Fig. 2 (b) – Simplified Cryptography Decryption

The simplified cryptography decryption is shown in the figure 2(b). The cryptography decryption retrieves original information with the help of public key.

III. Steganography

Steganography is an art of hide the existence of information by using the cover in such a way that, it looks like simple cover, though it has hidden information [7]. There are many different ways of performing steganography. In this paper, LSB of pseudo randomly selected pixels of selected frame of video is replaced by the information bit, to perform LSB based steganography. Simplified LSB replacement.

The Steganography encryption is design to replace LSB of only selected pixels [8], and the selection is made dynamic by keeping it dependent on the statically selected pixel information, frame number etc.

The encryption is also added with the feature that, in the first frame of the stego video itself, contains the information about hidden data, such as type of file format size of hidden information etc. The decryption will utilize this information and can extract out the hidden data from stego video.

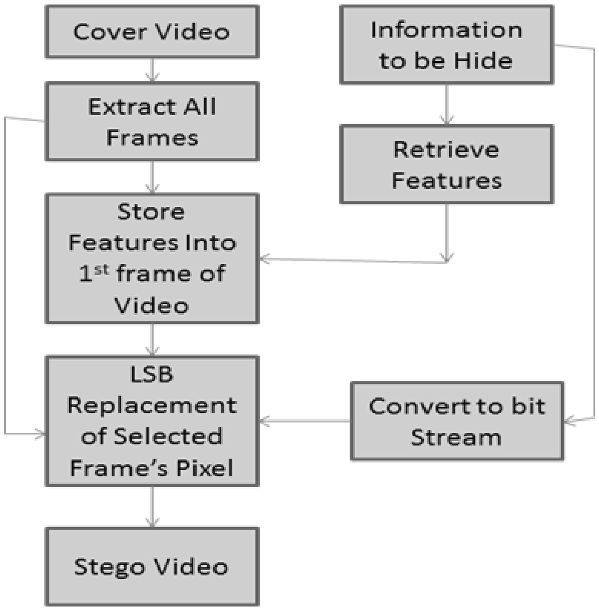


Fig. 3 (a) – Steganography Encryption

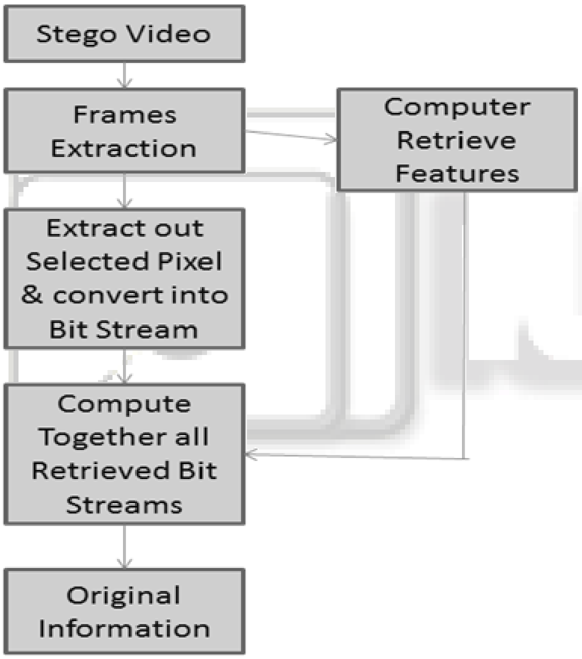

Stego Video
Frames Extraction
Computer Retrieve Features
Extract out Selected Pixel & convert into Bit Stream
Compute Together all Retrieved Bit Streams
Original Information

Fig. 3 (b) – Steganography Decryption

IV. Cryptography-Steganography

The proposed algorithm is to fuse the cryptography and steganography to hide the information. Initially, Information is converted into garbage information using cryptography, and then it is hiding inside the cover video using steganography; hence any steganalysis tools, cryptanalysis or brute force method is not able to find the hidden information.

The different cryptography algorithm used here are Caesar cipher, modified Caesar cipher, transposition cipher are used along with the LSB replacement based steganography to generate crypto-steganography.

Caesar cipher is the one of the simplest and most widely known encryption technique. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

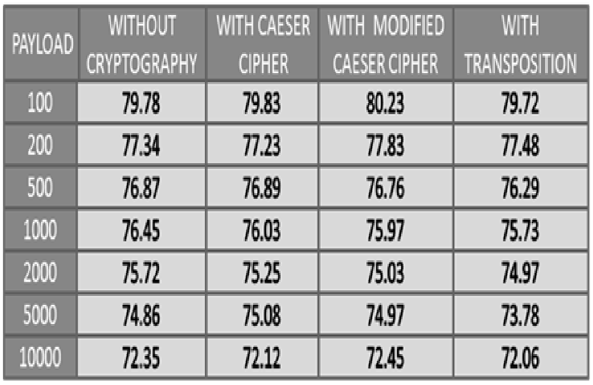
In modified Caesar cipher technique, key is used to create cipher message from original message. Based on length of original message, if key contains less elements then original message then padding will be used. Same key repeated up to the length of original message. If key contains more characters then plain text then characters of key are removed. Now according to key, message will be converted into cipher text.

In transposition cipher is methods of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a specific system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed.

V. Results and Conclusion

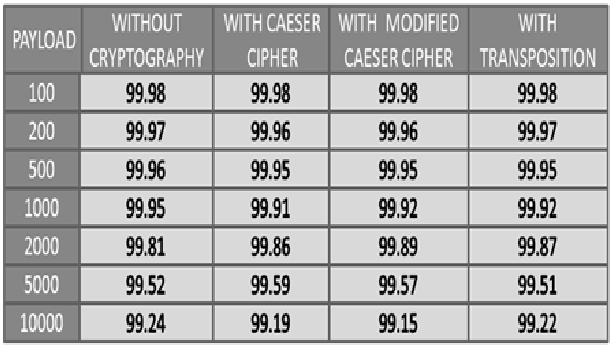
The various cryptography techniques are used along with the LSB replacement based steganography,to compute and generate various cryptography-steganography results. The cryptography-steganography are performed with various payload.

It can be seen from the result that, even after applying any of the cryptography algorithm, BCR and PSNR are remain almost same for all payload. The cryptography-steganography image is more secured compared to only steganography. The addon of the cryptography does improve security while keeping the BCR and PSNR almost same.



PAYLOAD	WITHOUT CRYPTOGRAPHY	WITH CAESER CIPHER	WITH MODIFIED CAESER CIPHER	WITH TRANSPOSITION
100	79.78	79.83	80.23	79.72
200	77.34	77.23	77.83	77.48
500	76.87	76.89	76.76	76.29
1000	76.45	76.03	75.97	75.73
2000	75.72	75.25	75.03	74.97
5000	74.86	75.08	74.97	73.78
10000	72.35	72.12	72.45	72.06

Table 1: PSNR result for various Crypto-Steganography
[PSNR (Peak Signal to Noise Ratio)]



PAYLOAD	WITHOUT CRYPTOGRAPHY	WITH CAESER CIPHER	WITH MODIFIED CAESER CIPHER	WITH TRANSPOSITION
100	99.98	99.98	99.98	99.98
200	99.97	99.96	99.96	99.97
500	99.96	99.95	99.95	99.95
1000	99.95	99.91	99.92	99.92
2000	99.81	99.86	99.89	99.87
5000	99.52	99.59	99.57	99.51
10000	99.24	99.19	99.15	99.22

Table 2: BCR result for various Crypto-Steganography
[BCR (Bit Correction Ratio)]

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