Indian Journal of Science and Technology, Vol 8(23), DOI: 10.17485/ijst/2015/v8i23/85289, September 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Video Steganography Based on Hash Polynomial Function for Secure Communication Use Fourier Transform with Security Method for Mounting of Multilayer Security

R. Umadevi[1*] and G. M. Nasira[2]

[1]Department of Computer Science, Periyar University, Salem – 636011, Tamil Nadu, India; mail2deviuma@gmail.com
[2]Department of Computer Science, Chikkanna Government Arts College, Tirupur – 641602, Tamil Nadu, India; nasiragm99@yahoo.com

Abstract

Now-a-days, several well-organized data hiding methods have been introduced and implemented using video steganography channel. Data hiding is to accomplish better data communication by hiding information into a video medium carrier to form an unrecognizable code stream. In the consideration of security aspect for communication process especially in video we enhanced this QoS factor security in this paper. Due to heavy packet loss, channel bit errors, video stego analysis have become a significant addition to the security aspects and are extensively developed as a complementary line to conventional security method. In this work, Fourier Transform With Security (FTWS) technique is applied for improve the security on video files in communication process. In this paper, a Secure Hash Polynomial Function to provide multi-layer security according to the modular additions and density functions is presented. Through the analysis of performance factor the security is important factor in our research. Finally, the simulation results evaluated by Video Quality Experts Group with parameter such as security with multilayered for 110 frames using MATLAB. It shows that the method FTWS enhance the security significantly compared with typical state-of-the-art methods.

Keywords: Fourier Transform, Hash Polynomial Function, Packet Loss, Security, Video Steganography

1. Introduction

In[1], steganography based on color histogram was introduced to guarantee integrity and improve the security for the images being extracted. With the objective of improving the security of data or images or videos being sent through Internet, Extended Substitution Algorithm (ESA)[2] was introduced to minimize the noise ratio for varying length of text messages. Another method in[3] integrated Advanced Encryption Standard (AES) and Discrete Cosine Transform (DCT) to improve the security of data being sent. Another security mechanism was introduced in[4] using Wavelet based Secure Steganography with Scrambled Payload (WSSSP) to significantly reduce noise ratio while sending cover image.

The significant advancement in processing multimedia file, the amount and content of digital data has become extensively large and widespread. As a result, several copies of digital data remain on the Internet, resulting in resource wastage. A mechanism was introduced in[5] that applied color correlation into non-overlapping blocks that significantly reduced the time and space complexity. However, temporal features according to color correlation were not included. Hash based Least Significant Bit

*Author for correspondence

technique (HLSB)[6] have introduced to address the temporal features to reduce the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) for video steganography. Robustness and security was addressed in[7] based on Discrete Cosine Transform (DCT). Data hiding using steganography techniques called, Spatial Domain based Graphic (DSG)[8] was introduced to address the issues related to security.

Based on the above said methods, an efficient method to improve the security using Fourier Transform is presented in the forthcoming sections.

2. Literature Review

The average prediction error rate also found and compared with our method in video quality is improved in the achieving secret communication on video files using steganography[9]. In the method, Multivariate Regression and Flexible Macro block Ordering[10] presented two data hiding technique to minimize the level of distortion using regression model. Though compression overhead was improved, robustness against channel bit errors was not resolved. Video Quality Assessment (VQA)[11] presented a scheme to measure the assessment of video streams with the aid of salient motion region segmentation. But, variance and intensity of temporal changes remained unattended. To consider the temporal changes, Least Significant Based Approach (LSBA)[12] was designed by applying edge adaptive scheme. This improved in obtaining high quality video images enhancing the security in a significant manner. Another method based on Vector Quantization (VQ)[13] was designed to reduce the peak signal-to-noise ratio using irreversible method with the advantage of reducing the compression rate. However, the spatial and temporal aspects were not taken into consideration.

In[14], a patch based technique was introduced to reduce the peak signal to noise ratio by introducing background tessellation and temporal clustering. However, spatial nature with respect to video sequence remained unaddressed. A steganography method called, Pixel Value based Differencing (PVD)[15] was introduced to provide better security using steganalysis improving the subject and object quality.

3. Overview of Proposed Method

The FTWS method achieves the great security measures in the field of communication. Figure 1 explains our method clearly. First selects the input as cover video then applies the irreversible rapid fourier transform to hide the secrete data and applying the secure hash polynomial function to get the secures stego video as output. This Figure 1 demonstrates to achieve the security by tapering the messages on multimedia files especially in video file.

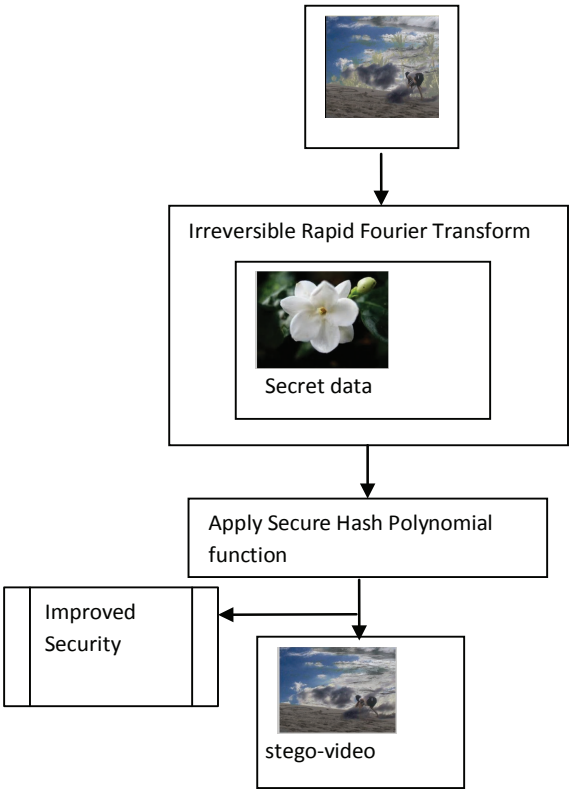

Figure 1. Block Diagram of FTWS.

In the video files timing is important factor for analyzing. Let us consider our input video files are split for executing method like VF1, VF2 …., VFn that are shown the Figure 2.

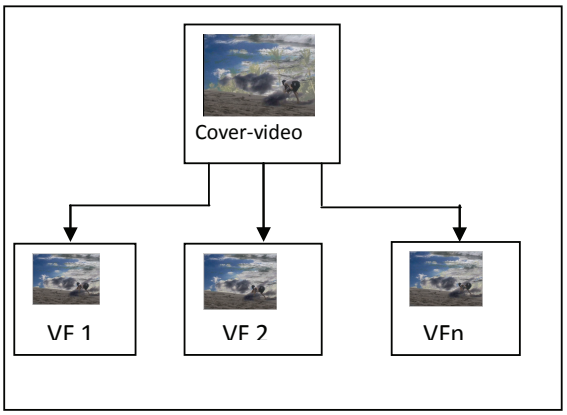

Figure 2. Split of video sequences.

By splitting of video sequences, the hash polynomial function applied for increases the security measures in the communications.

The algorithm describes the embedding and extraction process with our method of Fourier transform with security.

Input: cover-vide file, frames
Output: stego-video
//embedding
Begin
Step 1 For each cover-video file
Step 2 Select and split into video frames (VF1, VF2 ,,,, VFn)
Step 3 Convert secret message into cipher text using Secured Hash Polynomial Function.
Step 4 Transform the original frame with stego frame
Step 5 From (1) the robustness security measures calculated
Step 6 Get the secured form of stego-video
Step 7 End for
//extraction
Step 9 Input the stego-video
Step 10 Obtain FTWS for the secured stego-video
Step 11 Obtain secret messages and the cover-video file
End

The algorithm initially obtains the cover video file and split into frames by using hash polynomial function. The secret messages are hidden then the security measures formula is applied for achieving the better multilayered security.

4. Experimental Results

Security in Fourier Transform With Security (FTWS) measures the amount of noise during retrieval of secret data. The security is evaluated based on the ratio of difference between hidden secret data sent (i.e., in terms of size KB) and hidden message received. Higher the difference more securitized the method is said to be. It is measured in terms of percentage (%). The Table 1 values of Hidden Secrete Data send (HSD_S) and Hidden Secrete Data receive (HSD_R) are calculated and applied in the equation to get the robustness values then it is well compared for better understanding our proposed method.

Table 2 below shows the security for FTWS method, MRFMO and VQA versus six different secret data. The security over MRFMO and VQA increases gradually though not linear for differing video files for video steganography.

$$Robustness\ (Security) = \frac{(HSD_s - HSD_R)}{HSD_R} * 100 \quad (1)$$

Table 1. Security measures

Security (Using proposed FTWS) = (23.4 – 16.2) / 16.2 * 100 = 44
Security (Using MRFMO) = (23.4 – 16.5) / 16.5 * 100 = 42
Security (Using VQA) = (23.4 – 17) / 17 * 100 = 37

Table 2. Tabulation for security

Size of secret data (KB)	Security (%)		
	FTWS	MRFMO	VQA
23.4	45.3	43.15	38.2
25.4	49.5	46.25	43.15
43.3	43.85	40.25	38.25
51.2	41.25	38.15	33.15
65.3	58.22	43.25	40.13
82.5	62.15	51.25	45.15

Table 2 shows the security for FTWS method, MRFMO and VQA versus seven sizes of secret data in the range of 23.4 KB to 82.5 KB using different images. The security returned over MRFMO and VQA increases gradually though not linear for differing sizes of secret data for video steganography is observed.

From Figure 3, it is illustrative that the security is improved using the proposed method FTWS. For example, when the size of secret data was 23.4 KB, the security

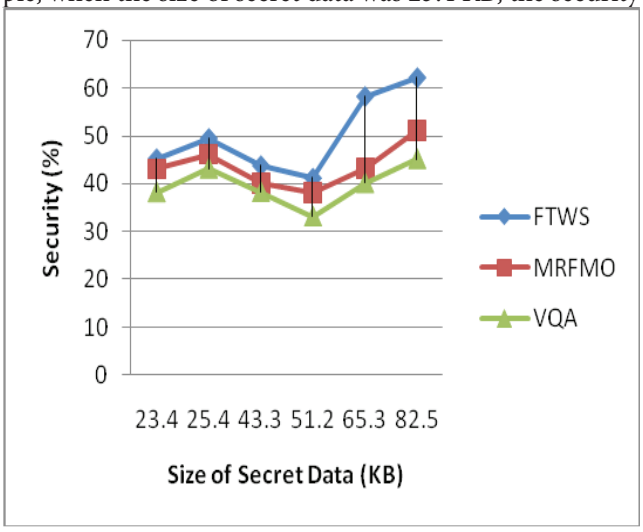

Figure 3. Measure of security.

obtained was 45.3 percent using FTWS method, 43.15 percent compared to MRFMO and 38.2 percent compared to VQA. Also with secret data size of 25.4 KB, the security achieved using FTWS method was 6.56 % better compared to MRFMO and 23.23 % compared to VQA respectively.

By observing the dense video frame behavior with differing size of secret data for video steganography, the security is ratio is improved. This is because with the application of bit distribution that sums the square value up below next value of frame and performs the same up to above next value of frame.

In the security concerns the values improved using our method is progressively increased but the measures are also may calculated for increasing size of secrete data. As the data hiding method ensures and promising way for the security measures and achieved better values.

5. Conclusion

With this, the security is improved in FTWS method ensures multi-layer security. Though the values can be accidentally discovered using FTWS method, using the hash polynomial values, the actual embedded secret data is not revealed, resulting in improved security. Therefore, Fourier Transform With Security (FTWS) technique is proposed to improve the security on video steganography based on variance and intensity of temporal changes.

The technique also addresses key challenges related to robustness on video files security according to the modular additions and density functions. Moreover the complexity is analyzed in the most of the quality factor but in this paper security factor is concentrated for increasing the safety measurement in the area of communication through the video files.

6. References

1. Kelash HM, Wahab OFA, Elshakankiry OA, El-sayed HS. Utilization of steganographic techniques in video sequences. International Journal of Computing and Network Technology. 2014 Jan; (1):17–24.
2. Gutte RS, Chincholkar YD, Lahane PU. Steganography for two and three lsbs using extended substitution algorithm. Ictact Journal On Communication Technology. 2013 Mar; 04(01).
3. Aung PP, Naing TM. A novel secure combination technique of steganography and cryptography. International Journal of Information Technology, Modeling and Computing (IJITMC). 2014 Feb; 2(1):55–62.
4. Reddy HSM, Raja KB. Wavelet based secure steganography with scrambled payload. International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2012 Jul; 1(2):121–9. ISSN: 2278-3075.
5. Lei Y, Luo W, Wang Y, Huang J. Video sequence matching based on the invariance of color correlation. IEEE Transactions on Circuits and Systems for Video Technology. 2012 Sep; 22(9):1332–43.
6. Dasgupta K, Mandal JK, Dutta P. Hash based least significant bit technique for video steganography. International Journal of Security, Privacy and Trust Management (IJSPTM). 2012 Apr; 1(2):1–11.
7. Singh S, Siddiqui TJ. A security enhanced robust steganography algorithm for data hiding. IJCSI International Journal of Computer Science Issues. 2012 May; 9(3):131–9.
8. Saha B, Sharma S. Steganographic techniques of data hiding using digital images. Defence Science Journal. 2012 Jan; 62(1):11–18.
9. Umadevi R, Nasira GM. Achieving secret communication on video files using steganography. IJCOA International Journal of Computing Algorithm. 2015 Mar; 4(Special).
10. Shanableh T. Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering. IEEE Transactions On Information Forensics And Security. 2012 Apr; 7(2):455–464.
11. Culibrk D, Mirkovic M, Zlokolica V, Pokric M, Crnojevic V, Kukolj D. Salient motion features for video quality assessment. IEEE Transactions On Image Processing. 2011 Apr; 20(4):1–11.
12. Luo W, Huang F, Huang J. Edge adaptive image steganography based on LSB matching revisited. IEEE transactions on information forensics and security. 2010 Jun; 5(2):201–14.
13. Wang Wei-Jen, Huang Cheng-Ta, Wang Shiuh-Jeng. VQ applications in steganographic data hiding upon multimedia images. IEEE Systems Journal. 2011 Dec; 5(4):528–37.
14. Colombari A, Fusiello A. Patch-based background initialization in heavily cluttered video. IEEE Transactions On Image Processing. 2010 Apr: 19(4):926–33.
15. Luo W, Huang F, Huang J. A more secure steganography based on adaptive pixel-value differencing scheme. Network Security and Cryptography. Springer; 2010 Jan.