An Enhanced and Secure Video Steganography Method Based on MOT and ECC

[1]Chouthri.S, [2]Vijayasuresh.M
[1]PG – Student, [2]Senior Assistant Professor
[1 & 2] Department of Electronics & Communication Engineering,
[1&2]Bharathidasan Engineering College, Nattrampalli, Vellore District, Tamilnadu, India.

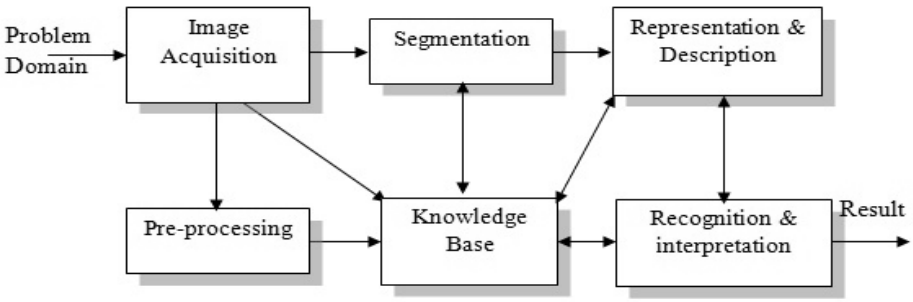
Abstract: Digital image data hiding techniques are increasing rapidly with the advancements in the field of digital image processing. Steganography and watermarking have gained extensive recognition. A tiny amount of data was embedded and hidden into a digital image, which can be retrieved with certain retrieval algorithms to confirm the secure transformation and copyright of a portion of digital information. In contrast, Steganographic techniques are widely used to hide a vast amount of data information secretly and securely into various harmless digital medium. In this paper, we propose to bring up to date data hiding techniques. A secure and safe video steganographic algorithm in Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) domains based lying on the Multiple Object Tracking (MOT) algorithm and Error Correcting Codes (ECC) is used. At initial level, motion-based MOT algorithm is employed to differentiate the portions of importance in the stirring objects. DWT and DCT were used to secure the data hiding process. The results were simulated using MATLAB 7.14, which represents the capability of embedding mechanism and also in opposition to various attacks.

Index Terms **- Multiple Object Tracking (MOT), Discrete Wavelet Transform (DWT), Digital Image, Steganography, Watermark Embedding.**

I. INTRODUCTION

A picture with 2 dimension is represented by a digital processor is termed as digital image. In general, digital image can be represented as an array of real or complex numbers with a finite number of bits. An image will be digitized and stored in computer memory as a matrix of binary digits. A collection of real or complex numbers with a finite number of bits comprises a digital image. The digitized image can be used for processing and displaying on a screen with a high-resolution. Conversion of an image into a numerical depiction which is fit for input into a computer is the process of digitizer. Few of the widely used digitizers are Microdensitometer, Flying spot scan, Image dissector, Videocon camera and photosensitive solid- state arrays. The elementary sequences involved in an image processing system are shown in Fig. 1.

Figure 1 Elementary Steps in Image Processing System



In common, digital image can be represented as an array of real or complex numbers with a finite number of bits. An image will be digitized and stored in computer memory as a matrix of binary digits. To claim ownership in digital media, a digital watermark can be used. In this paper, we propose a solution to overcome the ownership issues on any digital media. We incorporate biometric data and its features to provide secure ownership. Watermarks produced from biometric features are used to encrypt fingerprint images. In this way unique recognition can be achieved and ownership for digital content can be established. In this framework, we have shown the importance of digital ownership for digital content in communication. The next section provides the survey followed by proposed framework with results and discussions.

Watermarking and steganography are the two most widely involved in secure transforming of message in digital communication. In the next section, we discuss the various techniques and algorithms used in steganography and shown the results of our proposed methodology.

II. Related Work

Embedded watermarking is the robust and secure scheme of digital media communication. We have performed the analysis of various secure mechanisms and proposed an efficient solution to improve secure way of communication.

An approach for motion trajectories was analyzed [2]. The representation problems of motion trajectories in a highly informative way are analyzed. Their approach introduced a droplet-based process to exemplify the high-dimensional 3D tube information in an uncomplicated however efficient method. The algorithms which they have used had proved the effectiveness of their approach.

In paper [3], the most challenging visual object tracking was considered as the target objects frequently changes their appearance caused by warp, unexpected motion, background untidiness and occlusion. They make use of the features extract from deep convolutional neural networks trained on object recognition datasets to get better tracking correctness and strength. The proposed algorithms performance has proved its efficiency in the experimental results a large-scale benchmark dataset.

A new video steganography algorithm [4] which is based on the multiple object tracking algorithm and Hamming codes was proposed and used in four stages. In data communication, steganography plays a vital role in secure and secret data information exchange. Initially the message is preprocessed, and Hamming codes (n, k) are applied in order to generate an encoded message. Next a motion-based multiple object tracking algorithm is applied on cover videos. This is to recognize the portions of the moving objects. Then, the embedding process of the encoded message was performed. At last, the extraction of secret message process from the 1 LSB and 2 LSBs for every RGB component of all moving regions is accomplished. Their results are proved with a high embedding efficiency and payload.

A novel magic least significant bit substitution method (M-LSBSM) [5], for RGB images was proposed which is based on the achromatic component of the (HSI) color model and multi-level encryption (MLE) in the spatial domain. Steganography is booming as a research area where secret way of communication is much more growing day by day. MLE algorithm was followed to divide the I-Plane into 4 sub-images of equal size. Their results validates that their proposed method enhances the visual quality of stego images and also provides good quality imperceptibility and several security levels as compared to a number of existing well-known methods.

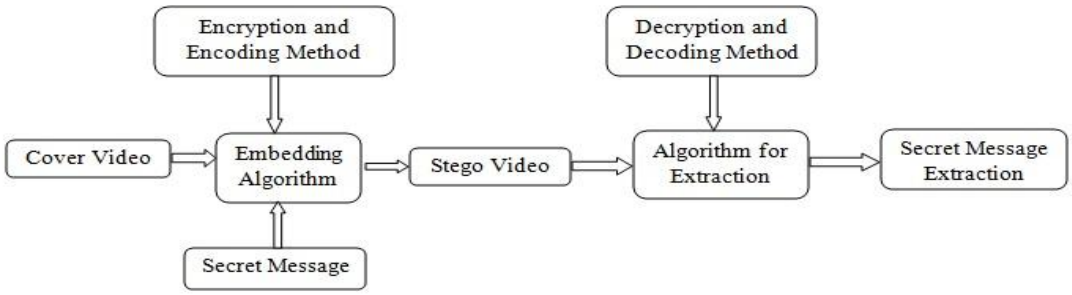
The issues with secure communication of susceptible contents over the public network are addressed in paper [7]. They came out with a novel data hiding method in encrypted images with dual-level security. A precise pattern was used to divide the secret data information into 3 blocks. Then the three-level encryption algorithm (TLEA) was followed for an encryption process. Their experimental results validate the effectiveness of the proposed methodology in terms of visual quality and security. It also guides the probability for safe communication of diagnostically important key frames to healthcare centers.

All the techniques utilizes the preprocessing stages for the exploitation on both secret messages and cover videos prior to the embedding phase in order to improve the security and robustness of the steganographic method. This needs an optimal solution to improve the effectiveness and to gain the bandwidth and also to formulate the system adaptive for different types of images based on their characteristics. An efficient scheme is widely needed to evaluate on a large set of images from various databases.

III. Proposed Work

The objective of our solution is to invent of an optimal wideband band pass filter to enhance the image properties. DE based dissimilarity augmentation in the direction of involuntarily locate the gain and the bandwidth of the WBBF toward formulate the scheme adaptive for dissimilar types of images based on their uniqueness. Laplacian of Gaussian response (LoGR) in 2 dimensional attributes space and also using Differential Evolution for the Maximization of mutual information. By Using these encryption methods and ECC will achieve a protected and strong steganographic algorithm. DWT and DCT techniques resolve get better strength of the steganographic technique against attacks, therefore preserves imperceptibility of stego videos. The proposed methodology was simulated using MATLAB 7.14. This integrates various computation and programming task and provides us an easy-to-use environment. This will be a better way to implement and simulate the solutions.

Figure 2 Work Flow Process of Proposed Scheme



3.1 Motion-Based MOT Stage

To identify the stirring objects within the video frame should be conceded away while motion object portion regions are utilized as host data. An individual frame is used to detect each moving object and then associating these detections throughout all of the video frames. To detect moving objects a background subtraction method is used based on the GMM. To predict the estimation trajectory of each moving region the kalman filter is employed.

3.2 Data Embedding Stage

To detect and track the motion regions motion-based MOT algorithm was performed over all video frames. The host data in the motion objects over all video frames are achieved. The interested portion in each and every individual frame depends on the number and size of the moving objects. 2D-DWT is implemented on RGB channels in every frame. These results in LL, LH, HL, and HH sub bands. In adding to this, a 2D-DCT is used on the similar interested portions producing DC and AC coefficients. After this, the secret messages are covered into LL, LH, HL, and HH of DWT coefficients, and into DC and AC of DCT coefficients of each objects in moving independently based on its foreground mask.

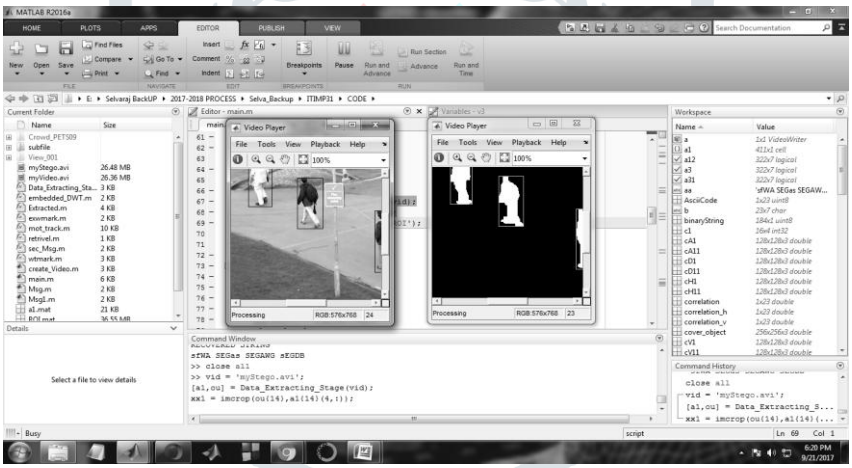
3.3 Data Extraction Stage

Two secret keys are generated from the non-motion portion of the first video frame and the video is broken up into a number of frames on the target side. The motion-based MOT algorithm is used by the receiver to predict the motion objects trajectories. By generating the secret messages from LL, LH, HL, HH, DC, and AC coefficients the process of extraction for the embedded data was achieved. Hamming and BCH was used to decode and extract the secret message and then the original message was encrypted.

IV. RESULTS

The input MOT image was shown in the below Fig. 3.

Figure 3 MOT Image



After getting the image, the watermark embedding process in initiated for secure transmission of information across sender and receiver. The original image will be embedded using DWT and later at the receiver side, the hidden information will be retrieve d securely and this was illustrated in Fig. 4.

The embedded watermarked embedded image will be retrieved on the receiver side and this was examined using a MATLAB Tool and the same was represented in Fig. 5.

Figure 4 MOT Image

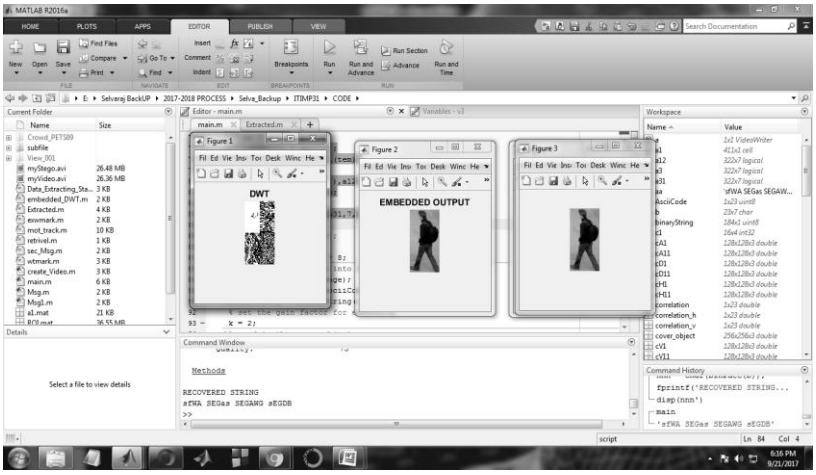
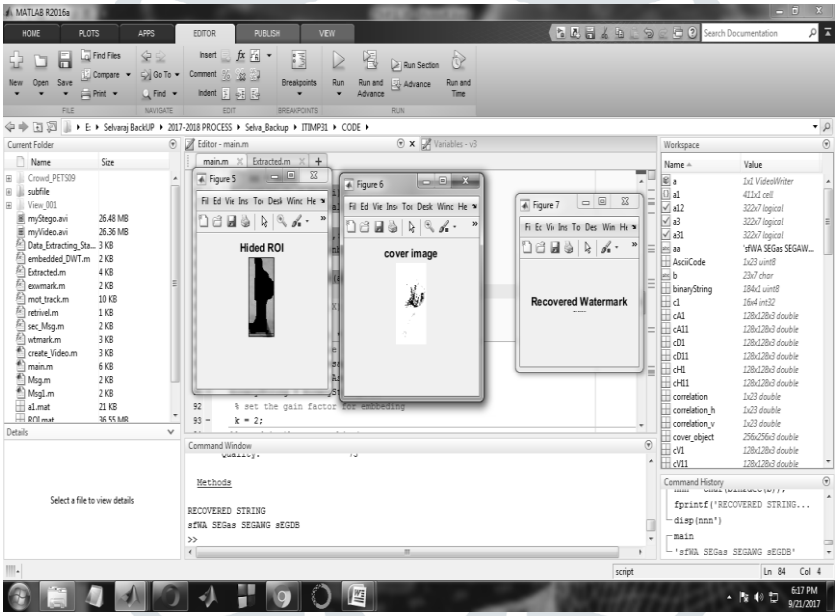


Figure 5 Recovered Watermark Image



V. CONCLUSION

`An efficient steganography method based on MOT and ECC in DWT-DCT domains was used in this paper. The proposed methodology utilizes the preprocessing stages as MOT and ECC, which leads to an enhanced confidentiality for the secret message preceding to embedding phase. We also validate the method of the method adjacent to various attacks; the security and robustness are achieved. We will use various efficient algorithms in several frequency domains to improve the efficiency, visual quality, and security. This will be addressed in our future work. Data hiding and secret way of communication was enhanced and made secure with our experimental results. We would also like to extend the implementation with various online tools in future.

REFERENCES

[1] RAMADHAN J. MSTAFA, KHALED M. ELLEITHY, AND EMAN ABDELFATTAH, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC", IEEE Trans., March 5, 2017.

[2] W. Lin et al., ``A tube-and-droplet-based approach for representing and analyzing motion trajectories," IEEE Trans. Pattern Anal. Mach. Intell., to be published.

[3] C. Ma, J.-B. Huang, X.Yang, and M.-H.Yang, ``Hierarchical convolutional features for visual tracking," in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Dec. 2015, pp. 3074_3082.

[4] R. J. Mstafa and K. M. Elleithy, ``A novel video steganography algorithm in DCT domain based on Hamming and BCH codes," in Proc. IEEE 37th Sarnoff Symp., Sep. 2016, pp. 208_213.

[5] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S.W. Baik, ``A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools Appl., vol. 75, no. 22, pp. 14867_14893, Nov. 2016.

[6] X.-Y. Wang, C.-P. Wang, H.-Y. Yang, and P.-P. Niu, ``A robust blind color image watermarking in quaternion Fourier transform domain," J. Syst. Softw., vol. 86, no. 2, pp. 255_277, Feb. 2013.

[7] K. Muhammad, M. Sajjad, and S. W. Baik, ``Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy," J. Med. Syst., vol. 40, no. 5, pp. 1_16, 2016.

[8] M. Sajjad et al., ``Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," Multimedia Tools Appl., vol. 76, no. 3, pp. 3519_3536, Feb. 2017.

[9] M. S. Subhedar and V. H. Mankar, ``Current status and key issues in image steganography: A survey," Comput. Sci. Rev., vols. 13_14, pp. 95_113, Nov. 2014.

[10] S. Islam, M. R. Modi, and P. Gupta, ``Edge-based image steganography," EURASIP J. Inf. Secur., vol. 2014, p. 8, Dec. 2014, doi: 10.1186/1687- 417X-2014-8.

[11] M. Hasnaoui and M. Mitrea, ``Multi-symbol QIM video watermarking," Signal Process., Image Commun., vol. 29, no. 1, pp. 107_127, Jan. 2014.

[12] R. J. Mstafa and K. M. Elleithy, ``A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in Proc. Long Island Syst., Appl. Technol., May 2015, pp. 1_7.

[13] C. Rupa, ``A digital image steganography using sierpinski gasket fractal and PLSB," J. Inst. Eng. (India), B, vol. 94, no. 3, pp. 147_151, Sep. 2013.

[14] R. J. Mstafa and K. M. Elleithy, ``Compressed and raw video steganography techniques: A comprehensive survey and analysis," Multimedia Tools Appl., pp. 1_38, 2016, doi: 10.1007/s11042-016-4055-1.

[15] K. Muhammad et al., ``A secure method for color image steganography using gray-level modi_cation and multi-level encryption," KSII Trans. Internet Inf. Syst., vol. 9, no. 5, pp. 1938_1962, 2015.

[16] A. K. Singh, M. Dave, and A. Mohan, ``Hybrid technique for robust and imperceptible multiple watermarking using medical images," Multimedia Tools Appl., vol. 75, no. 14, pp. 8381_8401, Jul. 2016.

[17] Y. He, G. Yang, and N. Zhu, ``A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service," AEU-Int. J. Elec- tron. Commun., vol. 66, no. 4, pp. 305_312, Apr. 2012.

[18] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, ``Robust and imperceptible dual watermarking for telemedicine applications," Wireless Pers. Commun., vol. 80, no. 4, pp. 1415_1433, Feb. 2015.