International Journal of Computer Science and Engineering Communications,
Vol.3, Issue.4, Page.1235-1239, (2015)
www.scientistlink.com

Data Hiding in Compressed Video using Motion Vector

[1] Mahalakshmi.S, [2]Subhashini.P

[1]PG Scholar - Department of Computer Science, St. Peter's University, Chennai, India.

[2]Assistant Professor- Department of Computer Science, St. Peter's University, Chennai, India.

[1]mahalakshmi.ramesh07@gmail.com, [2]subhait2k@rediffmail.com

ABSTRACT

Video data hiding is still an important research topic due to the design complexities involved. It propose a new video data hiding method that makes use of erasure correction capability of Repeat Accumulate codes and superiority of Forbidden Zone Data Hiding. Selective embedding is utilized in the proposed method to determine host signal samples suitable for data hiding. Video data hiding method also contains a temporal synchronization scheme in order to withstand frame drop and insert attacks. The proposed framework is tested by typical broadcast material against MPEG-2, H.264 compression, frame-rate conversion attacks, as well as other well-known video data hiding methods. The decoding error values are reported for typical system parameters. The simulation results indicate that the framework can be successfully utilized in video data hiding applications.

IndexTerms: *Data hiding, Encryption, Decryption Stegnography, Steganalysis, MotionVector.*

1. INTRODUCTION

Data hiding is the process of embedding information into a host medium. In general, visual media are preferred due to their wide presence and the tolerance of human perceptual systems involved. Although the general structure of data hiding process does not depend on the host media type, the methods vary depending on the nature of such media. For instance, image and video data hiding share many common points; however video data hiding necessitates more complex designs as a result of the additional temporal dimension. Therefore, video data hiding continues to constitute an active research area. Data hiding in video sequences is performed in two major ways: bit stream-level and data-level.

In bit stream-level, the redundancies within the current compression standards are exploited. Typically, encoders have various options during encoding and this freedom of selection is suitable for manipulation with the aim of data hiding. However, these methods highly rely on the structure of the bit stream; hence, they are quite fragile, in the sense that in many cases they cannot survive any format conversion or transcoding even without any significant loss of perceptual quality. As a result, this type of data hiding methods is generally proposed for fragile applications, such as authentication. On the other hand, data-level methods are more robust to attacks. Therefore, they are suitable for a broader range of applications. Despite their fragility, the bit stream-based methods are still attractive for data hiding applications. For instance, in the redundancy in block size selection of H.264 encoding is exploited for hiding data.

In another approach the quantization parameter and DCT (Discrete Cosine Transform) coefficients are altered in the bit stream-level. However, most of the video data hiding methods utilize uncompressed video data. Sarkar et. al proposes a high volume transform domain data hiding in MPEG-2 videos. They apply QIM to low-frequency DCT coefficients and adapt the quantization parameter based on MPEG-2 parameters. Furthermore, they vary the embedding rate depending on the type of the frame. As a result, insertions and erasures occur at the decoder, which causes resynchronization. They utilize Repeat Accumulate (RA) codes in order to withstand erasures. Since they adapt the parameters according to type of frame, each frame is processed separately RA codes are already applied in image data hiding. In adaptive block selection results in de-synchronization and they utilize RA codes to handle erasures. Insertions and erasures can be also handled by convolution codes as in. The authors use convolution codes at embedded however; the burden is placed on the decoder. Multiple parallel Viterbidecoders are used to correct resynchronization errors. However, it is observed. that such a scheme is successful when the number of selected host signal samples is much less than the total number of host signal samples. In 3-D DWT domain is used to hide data. They use LL sub band coefficients and do not perform any adaptive selection. Therefore, they do not use error correction codes robust to erasures. Instead, they use BCH code to increase error correction capability.

By means of simple rules applied to the frame markers, it introduces certain level of robustness against frame drop, repeat and inserts attacks. And it also utilizes systematic RA codes to encode message bits and frame marker bits. Each bit is associated with a block residing in a group of frames. Random interleaving is performed spatio-temporally; hence, dependency to local characteristics is reduced. Host signal coefficients used for data hiding are selected at four stages. First, frame selection is performed. Frames with sufficient number of blocks are selected. Next, only some predetermined low frequency DCT coefficients are permitted to hide data. Then the average energy of the block is expected to be greater than a predetermined threshold. In the final stage, the energy of each coefficient is compared against another threshold.

2. LITERATURE SURVEY

2.1. Watermarking Security:

Theory and Practice. This paper proposes a theory of watermarking security based on a cryptanalysis point of view. The main idea is that information about the secret key leaks from the observations, for instance, watermarked pieces of content, available to the opponent. Tools from information theory (Shannon's mutual information and Fisher's information matrix) can me assure this leakage of information. The security level is then defined as the number of observations the attacker needs to successfully estimate the secret key. This theory is applied to two common watermarking methods: the substitutive scheme and the spread spectrum-based techniques. Their security levels are calculated against three kinds of attack. The experimental work illustrates how Blind Source Separation (especially IndependentComponentAnalysis) algorithms help the opponent exploiting this information leakage to disclose the secret carriers in the spread spectrum case. Simulations assess the security levels derived in the theoretical part of the paper.

2.2 Secure Spread Spectrum:

This paper presents a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data. We advocate that a watermark should be constructed as an independent and identically distributed (i.i.d.) Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data. We argue that insertion of a watermark under this regime makes the watermark robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, re-quantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation) provided that the original image is available and that it can be successfully registered against the transformed watermarked image. In these cases, the watermark detector unambiguously identifies the owner. Further, the use of Gaussian noise ensures strong resilience to multipledocument, attacks.Experimental results are provided to support these claims, along with an exposition of pending open problems.

2.3 Forbidden Zone Data Hiding

Forbidden Zone Data Hiding is introduced in .The method depends on the Forbidden Zone (FZ) concept, which is defined as the host signal range where no alteration is allowed during data hiding process. FZDH makes use of FZ to adjust the robustness-invisibility trade-off .The mapping function in (2) states that the host signal is modified by adding an additional term, which is a scaled version of the quantization difference. In 1-D, this additional term is scalar, whereas in N-D host signal is moved along the quantization difference vector and towards the reconstruction point of the quantizes. Hence, embedding distortion is reduced and became smaller than the quantization error.In order to fulfill the requirement of mutual exclusion, the reconstruction points of the quantizes that are indexed by different m should be non-overlapping, which can be achieved by using a base quantize and shifting its reconstruction points depending on m, similar to Dither Modulation .A typical embedding function that uses a uniform quantize.

3. PROPOSED SYSTEM:

Data hiding in video sequences is performed in two major ways: bit stream-level and data-level. A new block-based selective embedding type data hiding framework that encapsulates Forbidden Zone Data Hiding (FZDH) By means of simple rules applied to the frame markers, we introduce certain level of robustness against frame drop, repeat and insert attacks.

3.1 Encryption module:

In Encryption module, it consists of Key file part, where key file can be specified with the password as a special security in it. Then the user can type the data or else can upload the data also though the browse button, when it is clicked the open file dialog box is opened and where the user can select the secret message. Then the user can select the image or video file through another open file dialog box which is opened when the cover file button is clicked. Where the user can select the cover file and then the Hide button is clicked so that the secret data or message is hidden in cover file using Forbidden Zone Data Hiding Technique.

3.2 Decryption Module:

Decryption module is the opposite as such as Encryption module where the Key file should be also specified same as that of encryption part. Then the user should select the encrypted cover file and then should select the extract button so that the hidden message is displayed in the text area specified in the application or else it is extracted to the place where the user specifies it.

4. VIDEO COMPRESSION

Video compression technologies are about reducing and removing redundant video data so that a digital video file can be effectively sent over a network and stored on computer disks. With efficient compression techniques, a significant reduction in file size can be achieved with little or no adverse effect on the visual quality. The video quality, however, can be affected if the file size is further lowered by raising the compression level for a given compression technique.

Different compression technologies, both proprietary and industry standards, are available. Most network video vendors today use standard compression techniques. Standards are important in ensuring compatibility and interoperability. They are particularly relevant to video compression since video may be used for different purposes and, in some video surveillance applications, needs to be viewable many years from the recording date. By deploying standards, end users are able to pick and choose from different vendors, rather than be tied to one supplier when designing a video surveillance system. Axis uses three different video compression standards. They are Motion JPEG, MPEG-4 Part 2 (or simply referred to as MPEG-4) and H.264. H.264 is the latest and most efficient video compression standard.

Block Diagram

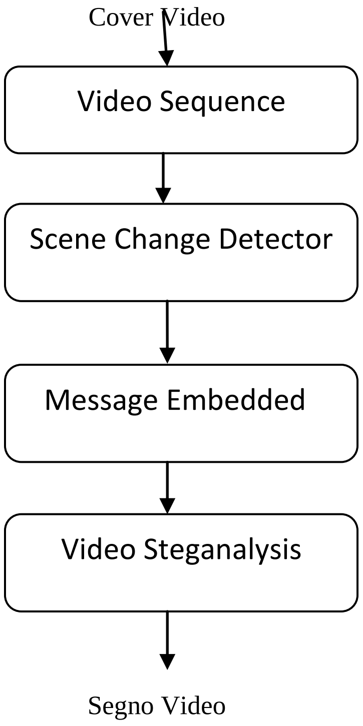

FIG-1. Block Diagram

4.1 Block Matching Algorithm

Block-based motion compensation takes into account that much of what makes up a new frame in a video sequence can be found in an earlier frame, but perhaps in a different location. This technique divides a frame into a series of macro blocks (blocks of pixels). Block by block, a new frame can be composed or 'predicted' by looking for a matching block in a reference frame. If a match is found, the encoder codes the position where the matching block is to be found in the reference frame. Coding the motion vector, as it is called, takes up fewer bits than if the actual content of a block were to be coded.

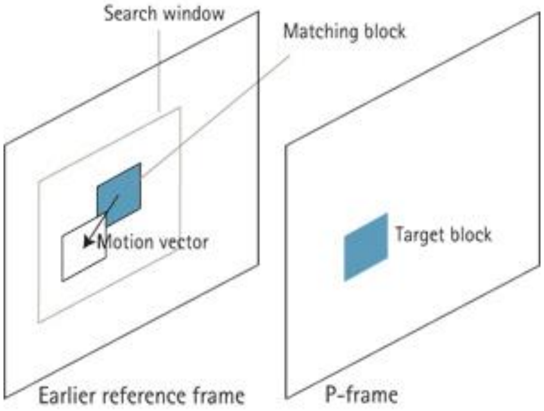

FIG-2 Block-based motion compensation.

With interframe prediction, each frame in a sequence of images is classified as a certain type of frame, such as an I-frame, P-frame or B-frame.An I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. The first image in a video sequence is always an I-frame. I-frames are needed as starting points for new viewers or resynchronization points if the transmitted bit stream is damaged. I-frames can be used to implement fast-forward, rewind and other random access functions. An encoder will automatically insert I-frames at regular intervals or on demand if new clients are expected to join in viewing a stream. The drawback of I-frames is that they consume much more bits, but on the other hand, they do not generate many artifacts, which are caused by missing data.

5. Algorithm Description

By construction, d*e= 1 mod φ(n). The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. (p, q, and φ(n) must also be kept secret because they can be used to calculate d.)

Encryption

Alice transmits her public key $(n, e)$to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that $0 \leq m < n$by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text $c$corresponding to

$$c = m^e \pmod{n}.$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits $c$to Alice.Note that at least nine values of m could yield a cipher text c equal to m,[5] but this is very unlikely to occur in practice.

Decryption

Alice can recover $m$from $c$by using her private key exponent $d$via computing

$$m = c^d \pmod{n}.$$

Given$m$, she can recover the original message M by reversing the padding scheme.

(In practice, there are more efficient methods of calculating c^dusing the pre computed values below.)

For efficiency many popular crypto libraries (like OpenSSL, Java and .NET) use the following optimization for decryption and signing based on the Chinese remainder theorem. The following values are precomputed and stored as part of the private key:

$p$and q: the primes from the key generation,

$d_P = d \pmod{p-1}$,

$d_Q = d \pmod{q-1}$and

$q_{Inv} = q^{-1} \pmod{p}$.

These values allow the recipient to compute the exponentiation $m = c^d \pmod{pq}$more efficiently as follows:

$m_1 = c^{d_P} \pmod{p}$

$m_2 = c^{d_Q} \pmod{q}$

$h = q_{Inv} * (m_1 - m_2) \pmod{p}$(if $m_1 < m_2$then some libraries compute h as $q_{Inv} \times (m_1 + p - m_2) \pmod{p}$)

$m = m_2 + (h * q)$

This is more efficient than computing $m = c^d \pmod{pq}$even though two modular exponentiations have to be computed. The reason is that these two modular exponentiations both use a smaller exponent and a smaller modulus.

8 CONCLUSIONS

The video data hiding framework that makes use of erasure correction capability of RA codes and superiority of FZDH. The method is also robust to frame manipulation attacks via frame synchronization markers. First, compare FZDH and QIM as the data hiding method of the proposed framework. We observe that FZDH is superior to QIM, especially for low embedding distortion levels. The framework is tested with MPEG-2, H.264 compression, scaling and frame-rate conversion attacks. Typical system parameters are reported for error-free decoding. The results indicate that the framework can be successfully utilized in video data hiding applications. Additionally, incorporation of Human Visual System based spatio-temporally adaptation of data hiding method parameters as in remains as a future direction.

6. REFERENCES

[1] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, “Data Hiding in H- 264 Encoded Video Sequences,” in IEEE 9th Workshop on Multimedia Signal Processing, MMSP 2007, pp. 373—376.

[2]A.Sarkar,U. Madhow, S. Chandrasekaran, and B. S. Manjunath, “Adaptive MPEG-2 Video Data Hiding Scheme,” in Proceedings ofSPIE Security, Steganography, and Watermarking of Multimedia Contents IX, 2007.

[3]K.Solanki,N.Jacobsen,U.Madhow,B. S.Manjunath, and S. Chandrasekaran, “Robust image-adaptive data hiding using erasure and error correction,” IEEE Transactions on Image Processing, vol. 13, Dec. 2004, pp. 1627--1639.

[4]M.Schlauweg,D.Profrock,andE.Muller,“Correction of Insertions and Deletionsin Selective Watermarking,” in IEEE International Conference on Signal Image Technology and Internet Based Systems, SITIS '08, 2008, pp.277—284.

[5] H.Liu, J.Huang, and Y. Q. Shi, “DWT-Based Video Data HidingRobust to MPEG Compression and Frame Loss,” Int. Journal of Image and Graphics, vol. 5, pp. 111-134, Jan. 2005.

[6] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt,” Digital image steganography: Survey and analysis of current methods Signal Processing”, 90 (2010),727–752.

[7] C.K. Chan, L.M. Chen, “Hiding data in images by simple LSB substitution”, Pattern recognition, 37 (3) (2004), 469–474.

[8] R.Amirtharajan, Adarsh D, Vignesh V and R. John Bosco Balaguru, “PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography”, International Journal of Computer Applications 7(9),(October 2010),31–37.

[9] R.O. EI Safy, H. H. Zayed, A. EI Dessouki, “An Adaptive Steganographic Technique Based on Integer Wavelet Transform”, International conference on Networking and media convergence ICNM-(2009), 111 - 117.