International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

An Infallible Technique for Hiding Confidential Data in Compressed Video using LSB and RSA Algorithm

Ismaila Idris, Onoja Emmanuel Oche, and John K. Alhassan
Department of Cyber Security, Federal University of Technology, Minna, Nigeria

***Abstract*—By hiding data in compressed video using a secret key, we can prevent and eliminate the security threat faced by computers and smart devices in this information age. In this paper, we hid data by focusing on the motion vectors used to structure and reframe both the frontward extrapolative and bi-directional in dense image frames. The selection of candidate set of these motion vectors are established on their affiliated prediction error. An adaptive threshold is sought for each frame (based on greedy approach) to gain lustiness while sustaining a modest error level. The secret data bit stream is inserted in the Least Significant Bit (LSB) of both parts of the candidate motion vectors. The approach is implemented and checked for hiding data in natural sequences of multiple blocks of frames and the outputs are measured. The measurement is based on minimum distortion to the reframed video and minimum overhead on the compressed video frame. The proposed approach is justified efficient in line the stated condition, and more valid when compare with a motion vector attribute-based approach.**

Keywords-confidential data; video Compression; data hiding Steg-analysis; watermarking; Huffman Codin; candidate motion vectors

I. INTRODUCTION

The term "Confidential data" typically denotes data classified as restricted, according to a specific data classification scheme needs to be properly secured via any secured mechanism that will not reveal it presence to an unauthorized party (steganography). This data hiding mechanism in different stegano-graphic cover is a broad field. It is a technique of embedding secret data in a media or other source and still maintaining the integrity of the data. It can be used to embed confidential information for annotation, access control, content transaction tracking, copy right protection and tampering detection [1].

This research focuses on internal changes of video compression process, precisely the motion estimation level. Choosing this level was based on the fact that the compressed video frames contents are internally processed during the encoding and decoding of the video which possess detection constraint when analyzed by applying image steg-analysis techniques besides it is coded loosely, thus it is not susceptible to quantization distortions. Change of motion vector based on Magnitude and Phase angle attribute has been the fundamental bases of most research applied on secure data hiding in a stegano-graphic cover. Confidential message in (data) bits are securely hidden in Motion Vector with high frequency above some specified $CMVs$

One data bit of the message is securely placed at the Least Significant Bit (LSB) of each larger Candidate Motion Vectors component, which is encoded as a unique area in a specified location generated by where the motion estimation generated motion vectors. Using the variable macro block 8 by 8, 8 by 16,16by 8 and16 by 16sizes of H.264, using each 2 bits from the data bit stream to choose one size out of the four different sizes for the Motion Estimation process. Carefully considering the angular (phase angle) difference between two nearest CMV, we embed the massage inside the sample video. These CMV were chosen according to the respective motion vectors magnitude. Using the Phase Angle Difference in sectors between CMV, the message bit stream is encoded accordingly with initial constrain of the block matching to search for a magnitude within the selected region to be greater than the initial threshold as predefined. This approach is focused on determining the direct reversible technique to find, at the decoder the CMV which relied on the motion vectors attributes.

Achieving least level distortion to prediction error and data size overhead was approached differently in this paper which is based on the prediction error associated with each block. The major constraint is difficulty of figuring out the non-linear quantization process.

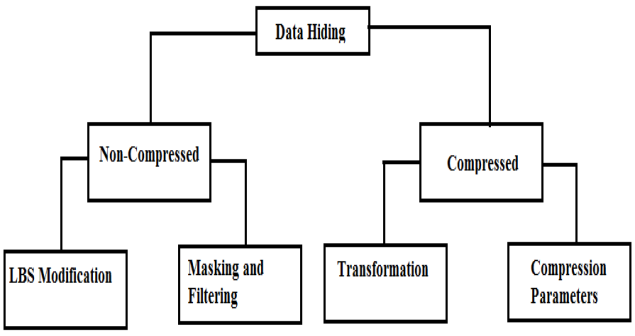

Figure 1. Data hiding techniques

II. RELATED WORKS

A mechanism of data hiding in compressed domain that makes use of encoding and compression sequences was proposed in [2], this is usually applied during different compression phase of after the compression phase of the

video sequences. An optimal output with less image distortions can me efficiently achieved when spatial and temporal model usually known as spatiotemporal model are concurrently used.

In [3], a data hiding technique based on transformation mechanism in which the Discrete Cosine Transform (DCT) coefficient modifications are done through sequential compression steps was proposed. The technique transforms a specified block of video frames (images) say 8 by 8 pixel block into a 64 DCT coefficients of separate values. A further systematic procedure is then carried out on the compression process; this is the quantization process, which is a usually based accurately calculated DCT coefficient. The secure data hiding procedure which is performed on the LSB of the frames immediately follow. It was observed that the above mechanism can be more secured if the encryption of secret data is done with pseudo-randomly generated secret key.

In [3], the frames' and macro-blocks' indices represent watermark which are embedded into the quantized DCT value of the blocks (the non-zero value). A watermarking process was used which is based on tampering detection technique. By using a semi-fragile watermarking protoco l the technique resulted in detecting temporal, spatial and spatio-temporal tampering region. After the DTC and quantization phases, follows the embedding process for some 4 by 4 block selected from each of 16 by 16 macro-blocks for embedding macro-block where the blocks with the larges Least Non Zero (LNZ) level arrangement are selected which simply define the frequency sample. For every selected block, 1 bit of message is embedded. The security of this mechanism was improved by using the secretkey A_s for authentication which is encrypted by a pseudo randomly generated key R_k to designate W_m the watermark point.

$$W_m = E(R_k : A_s) \qquad (1)$$

Another approach of securely hiding information was proposed in [4] where the coefficients' sign of some fundamental factors such as; the Motion Vector Difference (MVD), Intra Prediction Mode (IPM), and DCTare encrypted while data hiding is done on the DCT magnitudes at a specified threshold. The technique seems highly secure based on the fact that encryption process and data hiding mechanism were respectively done separately. This technique was mathematically modeled as precisely stated below, given that, watermark is represented as W_m and initial coefficient is of image Z, for every high security measure, q, encryption of watermark with a given a stream cipher before the process, we have the following:

Change in value of the coefficient is as:

$$z' = \begin{cases} z, if \ \lceil (\frac{|z|}{q}) \rceil \ \% \ 2 = 1 \\ X.q.Sign(z), z, if \ \frac{|z|}{q} \ \% \ 2 = 0 \end{cases} \qquad (2)$$

Where $X = \left(\lceil \left(\frac{|z|}{q} \right) \rceil + 1 \right)$

Otherwise,

$$z' = \begin{cases} z, if \ \frac{|z|}{q} \ \% \ 2 = 0 \\ X.q.Sign(z), z, if \ \frac{|z|}{q} \ \% \ 2 = 1 \ and \ z \neq -q \\ 2q.Sign(z), if \ z = -q \end{cases} \qquad (3)$$

Where $X = \left(\lceil \left(\frac{|z|}{q} \right) \rceil - 1 \right)$

In the work of [5], the Hide Behind Corner (HBC) algorithm was used to secretly hide message in which encrypted key is placed at the image corners and then the hidden image is convey via a stego-cover. The recipient of the message has a foreknowledge of all the encrypted keys hidden at the corner of the image. A reverse technique called Reverse Data Hiding (RDH) mechanism is applied to the encrypted image which contains the original message; this is only possible when all the encrypted corners are properly decrypted to using the appropriate secret key.

A new concept of data hiding using visual cryptography was presented in [6] where encrypted video is split into frames using FFMPEG tool. Randomly two frames are selected to hide secure message and image, converting this image to a grey scale and from grey scale to binary images which is then split into two shares using visual cryptographic scheme. The cipher text is embedded into the two shares. By using invisible watermarking technique, those two shares hidden in the selected frames and the image is hidden and finally all the frames are again converted into video using the FFMPEG tool and video is encrypted using the base64 encoder with asymmetric cryptographic technique. The receiver system performs video decryption accordingly, via a decryption splitting mechanism in which the system decrypts and split received video into separate units of frames and extracting various shares and data by selecting the frames which was watermarked

Another novel (and secure) data hiding mechanism was suggested by [7] in which embedding process of secret message in digital videos is performed based on magnitude of the phase angle of each motion vector(in the macro-block)found in each inter-frame. Selection of the candidate motion vector is based on an initialized threshold T. The mathematical representation of the phase angle in each motion vector for carrying out embedding process is calculated as follows:

$$\theta = arctan\left(\frac{MV_{iv}}{MV_{ih}}\right) \qquad (4)$$

Where;

MV_{iv} = the "vertical component of motion vector" MV_i

MV_{ih} = the "horizontal component of motion vector" MV_i

The mathematical steps for sequential data embedding are stated thus:

- For data bit = 0, search for MV_{2i} and MV_{2i+1} within the range of;

$$0^o < \theta_{2i} - \theta_{2i+1} \leq 180^o \qquad (5)$$

- For data bit = 1, t search for MV_{2i} and MV_{2i+1} within the range of;

$$180^o < \theta_{2i} - \theta_{2i+1} \leq 360^o \qquad (6)$$

- For all condition = Null, calculate a pair of motion vector that satisfied condition (i) and (ii) above.

In [8], a temporal model based on H.264 encoder was used for hiding data. In this model data hiding is based on Variable Block Sizes (VBS). The model standard uses seven un-identical but uniformly arranged block sizes 16 by16, 16 by 8, 8 by16, 8 by 8, 8 by 4, 4 by 8 and 4 by 4. The fundamental principle of this mechanism is to develop an encoder that will be forced to select a block type not just based on a single condition of efficiency alone but also on security parameters defined for the confidential data in respect available data integrity threat. This objective was achieved by assigning a randomly generated key in form of binary code to each separate block type. Each block has a unique binary code. For simplicity, a block of 4 by 4 sizes was used [10][11]. The security of this mechanism lies in the conversion process of the data before embedding process. Here, the data is change to binary digits, which are then grouped into various pairs and mapped into macro blocks which are going to be motion compensated and thereafter subjected to embedding process [13][14].

III. OVERVIEW OF PROPOSED SYSTEM

As shown in the figure below, the proposed confidential data hiding approach in compressed video using secret key has it input value as video. This input value is subjected to separation process in which the motion images (video) are split into image frames. The subjection process follows immediately, which subjects the image frames to coding process to produce a compressed frame (compressed video), where the coding procedure is DCT and Huffman coding. The next system stage is the application of secret key to the frames. With key generation principle based on RSA algorithm, a random secret key is generated, applied to the secret data which is then securely inserted to the video cover in the LSB of the frame through the implementation of LSB algorithm. This automatically produces the new video referred to as Stego-video. At the receiving end, the secret data can be extracted by reversing the LBS procedure and secret key process; this is also called inverse LSB and secret key.

A. *Algorithm Title: LSB Algorithm.*

Confidential data is embedding process is don on two separate pixels which are pixel$A$andpixel$B$as a cover for the confidential data respectively [15]. Adjustment process follows immediately on one of pixel A andpixel$B$ to embed 2bits of message $S_1$and message S_2. A flowchart representing the embedding process is represented in figure 3.

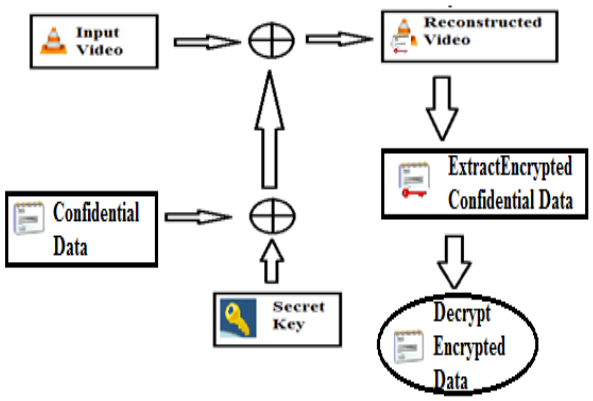

Figure 2. Proposed System

Step 1: For LSB of pixel A = messageS_1, go to second step2. And for, of pixel $A \neq$ messageS_1, go to step 3.

Step 2: For $f(A,B)$ = message S_2, all pixels remain unchanged. If the value of $f(A,B) \neq$messageS_2, pixel$B$ = +1 or -1

Step 3: For$f(A-1,B)$=messageS_2,pixel$A$= -1. And For $f(A-1,B) \neq$messageS_2; pixel$A$= +1

We mathematically state the function $f(A,B)$as;

$$f(A',B') = LSB\left(\left|\frac{A'}{2}\right| + B'\right) \qquad (7)$$

From the above algorithm, since the new LSB method for matching procedure is +1 or -1 based on pixel position, mostly the adjacent pixels and the separate pixel within the closet position between cover image tends to be very insignificant. We can infer that while hiding data high quality is maintained.

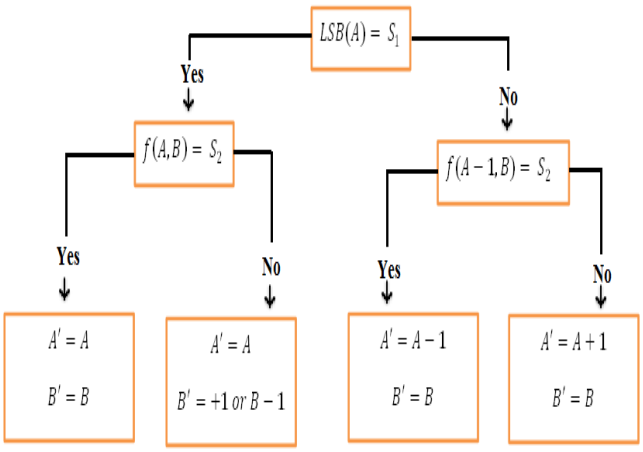

Figure 3. LSB Matching Embedding Procedure

B. *Algorithm Title: LSB Algorithm Data Hiding Algorithm*

This algorithm take input value as video and produce stego-video as output. It also implements other simple encoding procedures:

Step 1: Receive input value as video
Step 2: Perform separation process (video into frames)
Step 3: Perform8 by 8 block pixel Integer DCT
Step 4: Perform 8 by 8 block pixel scanning.
Step 5: By Huffman coding Compress frame
Step 6: Perform secret key and data encryption.
Step 7: Insert data to LBS
Step 8: Produce stago-video as output

C. Algorithm Title: Data Extraction Algorithm

This algorithm take input value as Stego-video and produce Hidden data (ciphertext) as output. It also implements other simple procedures.

Step 1: Take in Stego-video.
Step 2: Decoding step 1 via Inverse Huffman coding and IDCT.
Step 3: Perform inverse LSB and Secret Key to extract data.

D. Algorithm Title: KeyGeneration(RSA)Algorithm

Step 1: Randomly generate some large primes say p and q, nearer to a given key
Step2: Select a key within the range of p and q,
Step3: compute $n = p * q$,
Step 4: compute$m(p-1)(q-1)$
Step 5: Generate e

Assume $e = 1; x = 1$
While $(mod(m, e) = 0)$
$e = e + 1;$

Step 6: Generate d

Take $s = 1 + x * m$
While $(mod(s, e) = 0);$
$x = x + 1$
$s = 1 + x * m$
$d = s/e$

E. Our Greedy Search Algorithm

Our greedy search algorithm takes the following steps

Step 1: For 9 + 8 = 17 as overall points, check the points concentrated at the middle nine points including the product grid and the eight closest points to 9 * 9 grids. If the search window center =least block distortion point (Integer DCT), terminate search; if not, proceed to step 2.
Step 2: When the central 8closest points on the 3 * 3 grid is found to be the lowest in previous step, proceed to step 3; if not forward to step immediate step after step 3.
Step 3: Search until for winning point in step 1 above = 1 for window center in 3*3 searches. Search minimum of 3 based on position of winning point =1. Then halt search.
Step 4: Determine half of 9 * 9 search window sizes choose center to be equal to minimum block distortion measure point in step 1 and repeat search procedure as step 2 and step 3 in Three Search Step

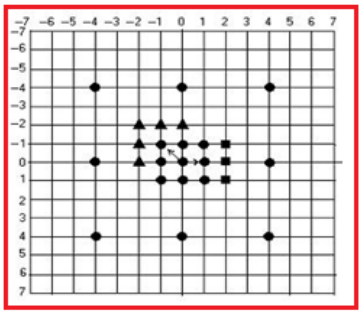

Figure 4. An independent two search paths for determining 5 * 5 MotionVectorwithina greedy search area

IV. EXPERIMENTAL RESULTS

A video stream of 89Mb was separated into three different frames, compressed, converted into binary codes using MATLAB) and subjected to message insertion (via LSB algorithm). The frames were reconstructed and an evaluation test of comparative performance of the re-constructed image frame (video) using size 256 X 256 for all frames from sample video was tested. With the transformation process on specific block size of 8 by 8, an optimum result of the DCT coefficient was obtained. This was found to be 64 coefficients. With the variation range of 1 and 64, the variousMSE and $PSNR$of the reconstructed image frames were compared with a defined standard image frame for different range of 1-64 as earlier used (i.e. excluding zero). The result obtained shows that data hidden in LSB of compressed video has little or no distortion to the original video. Based on the average PSNR estimation, a high PSNR value was obtained which proves high image quality of the reconstructed video which is similar to (if not almost the same as) the original video. At the receiving end, the whole insertion process was reversed. The experiment shows that concealed confidential data will be un-noticed even if the data is conveyed through an un-secured medium

Figure 5. Sample Ship Frames

As a criterion for good image quality, the parameter MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are express below;

MSE(Mean Square Error) is an acronym for the mean-squared error. It measures the error difference between a given stego-image and it covers [16]. This can be mathematically defined as follows:

$$MSE = K \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - Y_{ij}\right)^2 \quad (9)$$

Where

$$K = \left(\frac{1}{M*N}\right),$$

X_{ij} = Value of a given image in pixel at location (i, j) in the cover image

Y_{ij} = Value of a given image in pixel the same location in the fitting stego-image.

$$PSNR = 10\,E\left(\frac{(\text{Peak to peak value of the original data})2}{MSE}\right) \quad (8)$$

Where E= $\log_{10}$

The standard unit of measuring PSNR is usually designated as dB value for quality consideration. This means high value of PSNR signifies good quality of image

TABLE I. ANALYSIS OF PSNR VALUES FOR DIFFERENT TEST SEQUENCES

Experiment Setup		PSNR values of Original Information Image /extracted Image
Test sequence	Search Method for Motion Estimation	
Ship 1 (550B /frame) (33 frames)	Greedy Search	7.1583
Ship 2 (550 B /frame) (33 frames)	Greedy Search	13.9593
Ship 3 (550 B /frame) (33 frames)	Greedy Search	5.9047

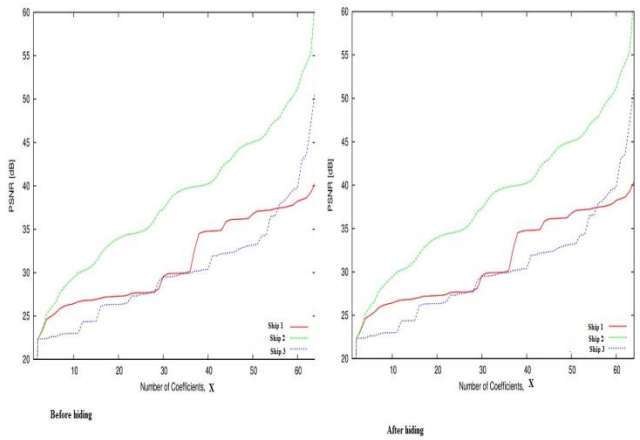

Figure 6. Graph of PSNR Sequence

From the PSNR sequences graph, the sequence of Ship1 and Ship 3 has high motion dynamics while Ship 2 has moderate upper finger motion. We evaluated this algorithm and compared PSNR value of original information image versus extracted image for different input videos

V. CONCLUSION AND FUTURE WORK

We were able to come up with an unfailing, optimally secure technique for hiding confidential information in a stego-medium. The above work still further it experiment via a three step greedy search process to choose a suitable value for threshold to be used in selecting macro-blocks that match to a given CMV in order for identically identified of candidates the decoder in-spite of the condition that a macro-blocks is not strongly compressed. The extraction of embedded image was found to be easy with almost no distortion to original message (massage integrity was absolutely maintained). This approach was compared with other massage hiding techniques gathered from different literatures and it was found more efficient, robust and reliable. Future work will focused on further increase in size of the "embedded payload" while maintaining efficiency, robustness and message integrity.

REFERENCES

[1] K. S. Anooplal and S.Girish "An infallible method to transfer confidential data using delta steganography", International Journal of Engineering Research and Technology (IJERT), vol.4, pp. 1060 – 1063, 2015.

[2] M. P. Hemalatha, R. Dinesh Kumar andD. Vinoth kumar "Image steganography using HBC and RDH technique", International Journal of Computer Applications Technology and Research,vol. 3, pp. 136-139, 2014.

[3] I. E. G. Richardson, "H.264 and MPEG-4 Video Compression: VideoCoding for Next Generation Multimedia". Hoboken, NJ, USA: Wiley, pp. 260 – 273, 2014.

[4] A. A. Hussein,"Data hiding in motion vectors of compressed video based on their associated prediction error",IEEE Trans. Inf. Forensics Security, vol. 6, pp. 100-120, March 2011.

[5] F. Mehdi, S. Shirmohammadi, M. Semsarzadeh, and J. Zhao,"Tampering detection in compressed digital video using watermarking" IEEE Trans. Instrumentation and Measurement, vol. 63, pp. 65-70, May 2014

[6] S.M. Poonkuzhali, "Data hiding using visual cryptography for secure transmission", International Journal of Advanced Research in Computer and Communication Engineering, , vol. 2, pp. 66-75, April 2015

[7] K.. Spyridon, , E. Eleni, N. Athanassios, V.Manjula, and K..Radhika "Data hiding in H.264 encoded video sequences", IEEE Proc. MMSP 2012

[8] S. G. Lian, Z. X. Liu, Z. Ren and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms," IEEE Trans. Consumer Electron., vol. 52, pp. 621-629, May 2014

[9] M. Shahid, Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames," IEEE Trans. Circuits Syst. Video Technol. Article in a conference proceedings: vol. 21, pp. 565-576, May 2011

[10] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," IEEE Trans. Inf. ForensicsSecurity, vol. 7, pp. 455–464, Apr. 2012

[11] S. E. Thomas, S. T. Philip, S. Nazar, A. Mathew and N. Joseph, "Advanced cryptographic steganography using multimedia files", International Conference on Electrical Engineering and Computer Science (ICEECS), pp. 239-242, May 2012.

[12] P. N. Ghorpade, " Data hiding in compressed video using LSB algorithm", International Journal of Engineering Research & Technology (IJERT),vol. 3. pp. 346-349, April, 2014.

[13] M. N. Asghar and M. Ghanbari, "An efficient security system for CABAC bin-strings of H.264/SVC," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 3, pp. 425–437, Mar. 2013.

[14] D. Angadi, R. Pimpale, Y. Vibhute and B.S.Kamble. "Data hiding in motion vectors of compressed video", International Journal of Emerging Technology and Advanced Engineering, vol. 4, pp. 234-239, February 2014.

[15] E. Diana and G. S. Jenifer, "Encrypted data hiding in video stream using code word substitution", International Journal of Science Technology & Engineering -IJSTE , vol 1, pp. 39-45, March 2015.

[16] R. Sridevi, V. L. Paruchuri, and K.S. Rao, "Image steganography combined with cryptography", International Journal of Computers & Technology, Vol.9, pp. 976-984,July2001.