

Robust Watermark Hiding Against Frame Dropping and Swapping Attacks

Israa Hadi Ali and Safa S. AL-Murieb
IT College, Babylon University, Hillah, Iraq

Abstract: As a result of the evolution of the means of communication and to protect the transmission of data over the internet and communication channels, the data of the media such as a video needs for protection and security. To provide that, a watermark will be added throughout the video but it is better to be hidden in different location in the frames not in fixed places nor in the background of frames. In this study a blind watermark embedding scheme was explained, by concealing different data in frames instead of embedding the same data. By embedding in most active object, another object was used as guiding to knows the bits that were hidden at each pixel of that object. Instead of hiding the same number of bits from watermark at every pixel of an active object, variation number of bits were concealed according to a homogeneity of a pixel with its neighbors. Also this study indicates how the proposed technique resists frame dropping and swapping attack, although of splitting the watermark into blocks and concealing each block in a frame.

Key words: Information hiding, copyright protection, watermarking, lsb, information security, content authentication, frame dropping attack, frame swapping attack

INTRODUCTION

In communications means, the transferred data may be stolen or changed when the sender sends his/her information to other parity. Thus, in order to secure and protect the data of the media that can be as a file of text, image, audio, or video, owner's mark is added to the media to ensure preservation of original information (Komal *et al.*, 2013). For satisfying data securing and protecting, there were many techniques such as steganography, cryptography and watermarking where each one has its characteristics and appropriate applications in wide range of data transitions (Gupta, 2014; Wayner, 2002).

Cryptography is a method of protection by converting the original data of the sender to another form that is non-readable for the foreign person (Gupta, 2014; Gupta *et al.*, 2014) while there is another different preserving method which means concealing a certain information which is in a digital form (like text or picture) to preserve the absence of information, this is named watermarking (Gupta *et al.*, 2014; Bhattacharya *et al.*, 2006). Steganography is a schema of writing a data such as any digital signal (audio file, image, text and video) in another signal that is called a cover (Gupta, 2014).

Related works: There were many researches about provide ability of copyright protection and authentication of the content and data of the media, Chan *et al.* (2004) proposed a scheme based on detecting changes in scene,

by scrambling the watermark into different parts and hiding same part of watermark in the frames of one scene. This was made robust against dropping the frames while the different parts were hidden in different scenes. Sanghavi proposed a method to conceal the watermark only in key frames after identifying such frames, firstly generating Fibonacci sequence that was used to choose frames for embedding. This approach had robustness against frame averaging and dropping.

Abinaya and Elango (2014) introduced a watermarking scheme for copyright protection in video, by hiding two watermarks, they were resistance watermark that was robust against frame dropping and rescaling, this watermark was embedded in spatial domain. While another watermark was semi fragile which was embedded in frequency domain using DWT.

Essaouabi *et al.* (2009) and Masoumi and Amiri (2012) analyzed and detected change of scene to conceal watermark in frames of motion scenes, watermark was embedded in the coefficients of DWT (LH, HL and HH bands). It was resistant to attacks such as frame swapping, averaging and dropping.

Shojanazeri *et al.* (2013) reviewed techniques of video watermarking for satisfying copyright protection and authenticating the content and data of the media, by showing the techniques of hiding at frequency domain (such as DCT, DFT and DWT transforms), at spatial domain (such as LSB, correlation based methods). With showing the attacks that were been resisted for these techniques.

Information hiding: The popularity of communications and internet and unreliability of media were the reason for securing, protecting and authenticating the source data during the transmission operation. The watermark identifies owner of the data without any ambiguous in extraction that watermark Embedding the data of authenticity means concealing information (such as owner's mark) in the original data, with the importance that isn't perceptual and doesn't influence the nature of perception (Bhaumik *et al.*, 2009; Katzenbeisser and Petitcolas, 2000).

The reasons behind hiding or concealing concepts are: personality's preserving and insure data privacy, critical data, data's abuse avoidance, preventing data elimination and any modification and others (Gupta *et al.*, 2014). In watermarking technique, it is preferred to embed invisible watermark across the digital multimedia (it hasn't been seen or percept), if the watermark is difficult in detecting or deleting it and if it is resistant to attack, this is called robustness, the amount of watermark data that was been hidden is called payload or capacity (Mauro *et al.*, 2005).

In order to protect digital data from unauthorized use, it is necessary to hide privacy data for many reasons, such as for copyright protection by embedding digital message (i.e. watermarking). Also, in order to prevent anyone knowing about existence of information or message, this is called steganography.

Watermark hiding can be applies in two different domains, spatially such as LSB method, or frequently using transformation that convert the digital data form from spatial to frequency domain (like DCT, DFT and WT) whereas watermark embedding is done in the coefficients of these transforms.

According to the watermark's perceptual, it can be completely seen, this is called visible mark such as logo, or it isn't seen, this is invisible, the applications of second kind are authentication, copyrighting, etc. According to the watermark's resistant, it is called fragile if it fails to be detected after the simple modification while a watermark is called semi-fragile, if it fails in detection after malignant

transformations although it resists beginning transformations and a watermark be robust if it withstands a designated class of transformations.

The watermarking systems can be non-blind, this is means that original cover must be exist in detection operation of the watermark to help of knowing the position of it in the watermarked cover, this type is also called private watermarking. Watermark can be semi-blind which doesn't need the original cover but it requires the watermark. It can be blind which means that both original cover and watermark are not required, it also called public watermarking (Chu *et al.*, 2009).

Proposed system: This study focuses on proposing adaptive algorithm to hide watermark in a video object, before hiding it is necessary to detect and track all objects throughout the frames of video, extract the trajectory for each object and select the most two active object as indicated in study (Chu *et al.*, 2009). After determining the most two active objects (called host and reference objects) based on the shapes of extracted trajectories that implement the movement of objects throughout the frames of video, the watermark will be concealed in the object corresponds to most complex trajectory. The general block diagram of the proposed work is clarified in the Fig. 1.

The proposed algorithm of watermark concealing in video media depends on dividing the data of watermark image into several blocks and each block will be concealed in a frame, therefore the number of frames that are required to hide all the block of watermark image for once time is equal to number of blocks of the watermark. The watermark is repeated many times, the maximum number of watermark repetitions is determined according to the following Eq. 1:

$$NRW = \frac{NF}{NB} \tag{1}$$

Whereas:

- NRW = The number of repetition of watermark
- NF = The number of total frames of the video
- NB = The number of blocks of the watermark

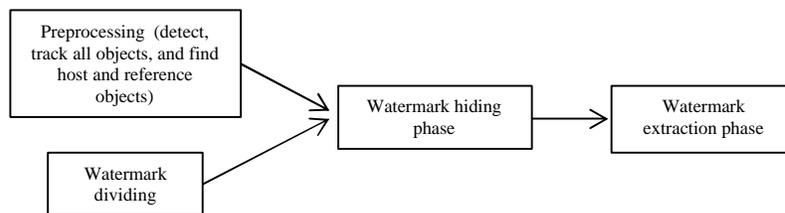


Fig. 1: General block diagram of the proposed system

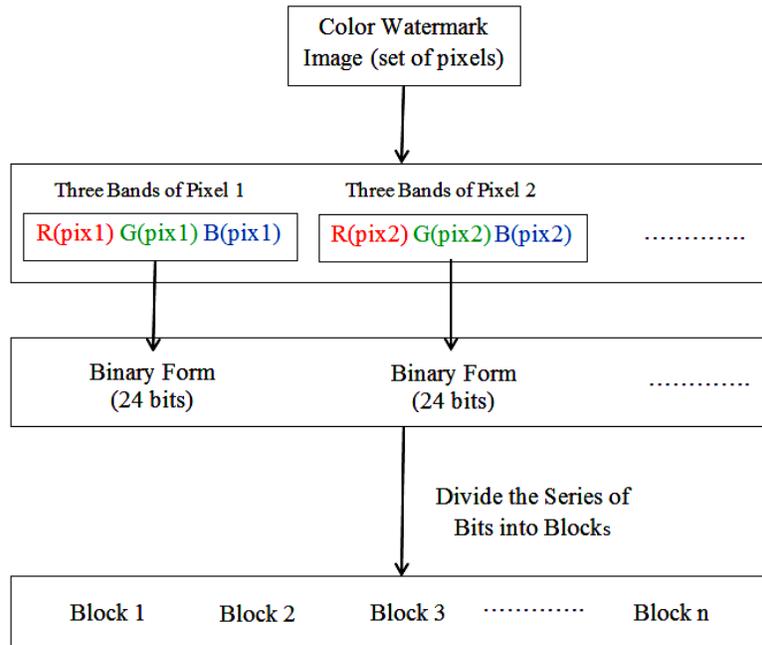


Fig. 2: Steps of dividing watermark image to blocks

The steps of dividing the watermark into blocks are:

- Separating each pixel in watermark into three bands (RGB) whereas the watermark image is color (i.e. each pixel exploits 24 bits)
- Then converting these color bands into binary form
- Dividing that series of bits into several blocks

The following figure demonstrates how to divide the watermark image data and equip it for concealment. In the published study (Ali and Murieb, 2015), the watermark was entirely concealed in each frame, whereas the main idea of concealing algorithm (by adapting LSB method) depends on hiding the watermark in the object that has the most motion activity. Hiding the watermark entirely in each frame means the embedded data in each frame is the same, this makes the frame dropping and swapping attacks have no effect to the extracted watermark because the watermark was embedded in each frame.

In order to hide different data in frames, the watermark's data will be divided into blocks (Fig. 2) and hiding a block in each frame. This makes frame dropping and swapping attacks effect the extracted watermark because in dropping attack, some frame will be lost, this causes losses of concealed blocks in such frames. While in swapping attack, there is no loss in any block but it causes incorrect sequence in extraction the blocks of watermark.

This study focuses on the proposed algorithm of hiding the blocks of watermark, whereas the effects of frame dropping and swapping attacks were been decreased and avoided consecutively although of hiding a block of watermark (not entirely) in each frame. Figure 3 shows the block diagram of hiding a block of the watermark in a frame of video.

In the proposed blind hiding algorithm, different number of bits were hidden in the host object (in the Least Significant Bit part of its pixels), instead of concealing fixed number of bits in each pixel of host object. So that with hiding modified number of bits, this means that the LSB based hiding algorithm is adapted, it is denoted as ALSB (Adaptive Least Significant Bit).

Every time, for hiding in every pixel of host object, it is needed to determine the number of bits of a watermark's block that will be hidden. Number of bits are specified according to the homogenous among the current pixel and its eighth neighbors.

When the deference between the current pixel and the average of its eighth neighbors is zero or one, this means that the homogeneity here is high, thus, one bit can be hidden. While when that deference increases, then two or three bits as maximum can be hidden as follow:

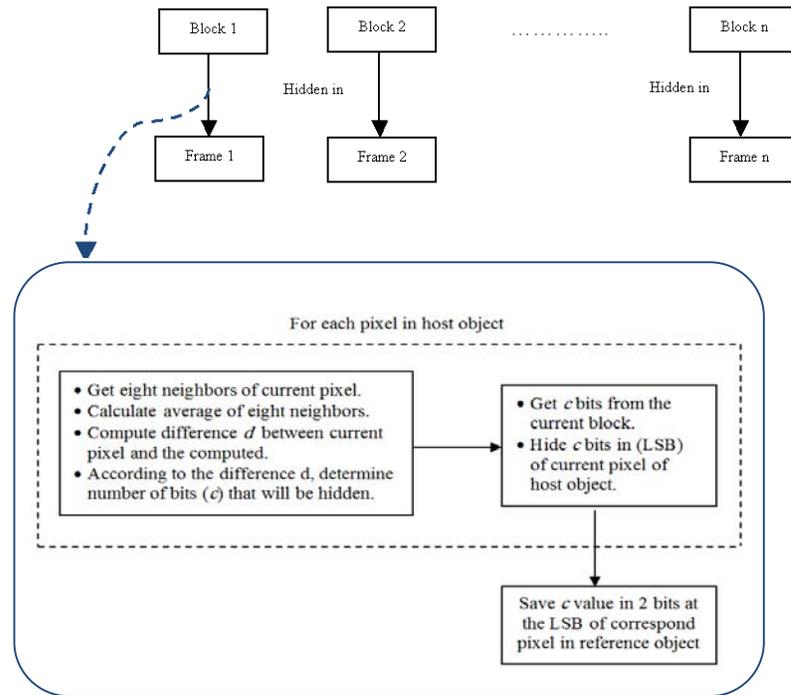


Fig. 3: Block diagram of hiding a block of watermark in a frame

If difference is 0 or 1 then
 Hide one bit of a block
 Else If difference is 2 or 3 then then
 Hide two bits of a block
 Else If difference is greater than or equal to 4
 Hide three bits of a block

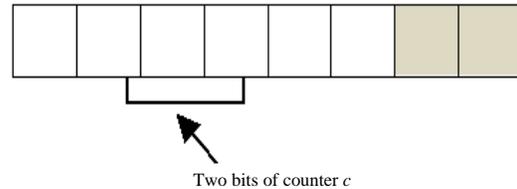


Fig. 4: Two bits of counter in corresponding pixel of the reference object

The main idea of concealing algorithm is hiding each watermark's block in an object of a frame, that object has the most motion activity. The most active object was denoted by host object and the second active object was denoted by reference object. Active object means that the shape of object's trajectory has many curvatures, the method of how these two object are selected was illustrated in detail in (Israa *et al.*, 2016).

After hiding number of bits (let it c bits) from a block in a pixel of host object, the value of number (c) will be saved in the 2 bits of LSB part of its corresponding pixel in reference object. This is used in the watermark extracting operation to know how many bits were hidden in each pixel of host object. Where the 2LSB of each corresponding pixel of reference object will be checked, this guides in finding the hidden bits of watermark within the host object to extract the watermark' block from each frame of video (Fig. 3).

Figure 4 indicates the position of storing the counter number (c) in the two bits at LSB part of corresponding

pixel in reference object. This number implements as guider to know the number of embedded bits in each pixel and it will be used in extracting the watermark's block from the host object from every watermarked frame.

In this proposed concealing method, each block of watermark is embedded in an object of video instead of embedding it in the background or stable position in the frame. The following algorithm describes the watermark hiding algorithm for one time, it is repeated many times to hide the watermark more than once where av in the algorithm is an average of 8-neighbors of current pixel and p is the current pixel This algorithm is used after detecting and tracking all objects that appeared in the frames of video and determining which are the most two active objects (host and reference objects).

Algorithm Name: Watermark Concealing.

Input: AVI Video file, colored watermark BMP image.

Output: Watermarked video (invisible watermarking).

Begin

- Step 1: Separate video file to set of frames (.BMP).
 - Step 2: Separate the pixels of watermark into their RGB bands.
 - Step 3: Convert the bands of step 2 into binary form.
 - Step 4: Divide the bits of step 3 into number of blocks (NB).
 - Step 5: For each block B of NB blocks, work with current frame
 - Step 6: For each pixel p in host object while there are block's bits don't be hidden do
 - Step 7: Obtain the 8-neighbors of the current pixel that surround it.
 - Step 8: Calculate the difference d between average of 8-neighbors and current pixel using $d = \text{abs}(av - p)$
 - Step 9: If $d = 0$ or 1 then c is 1
 else If $d = 2$ or 3 then c is 2
 else If $d \geq 4$ then c is 3
 - Step 10: Hide c bits from current block B in Least Significant Bit (LSB) of host object.
 - Step 11: Store number c in the 2bits of the LSB of reference object.
 - Step 12: End // For each pixel
 - Step 13: Set current frame to next frame.
 - Step 14: End // For each block
- End

After hiding a block in a frame, some additional information will be stored in the pixels of the frame's border, these information are useful for extraction process of the watermark in case of frame dropping and frame swapping. The information are:

- Number of current frame
- Number of watermark's block
- Number of the repetition of watermark

To extract the embedded block of watermark, the original cover doesn't used (it is blind scheme), so that

retrieval process is done by checking the two bits in LSB part of each pixel in reference object. According to the contents of these two bits the number of bits of watermark's block that were been hidden in the corresponding pixel in the host object, will be known, as the following:

If the value of two bits in LSB of the current pixel of reference object is 1

Then get one bit of LSB from the corresponding pixel in host object

Else If the value of two bits in LSB of the current pixel of reference object is 2

Then get two bit of LSB from the corresponding pixel in host object

Else If the value of two bits in LSB of the current pixel of reference object is 3

Then get three bit of LSB from the corresponding pixel in host object

With repeating this process to the all pixels in reference object, the bits of embedded watermark's block will be grouped and finally retrieving and extracting a block of the watermark. The following figure explains the retrieving of a block of watermark (i.e. from a frame) and by iterated it to extract all the blocks of watermark from the frames which were concealed within them.

By repeating the steps of that block diagram, each block will be extracted, the following algorithm explains the extraction process of the watermark entirely (Fig. 5).

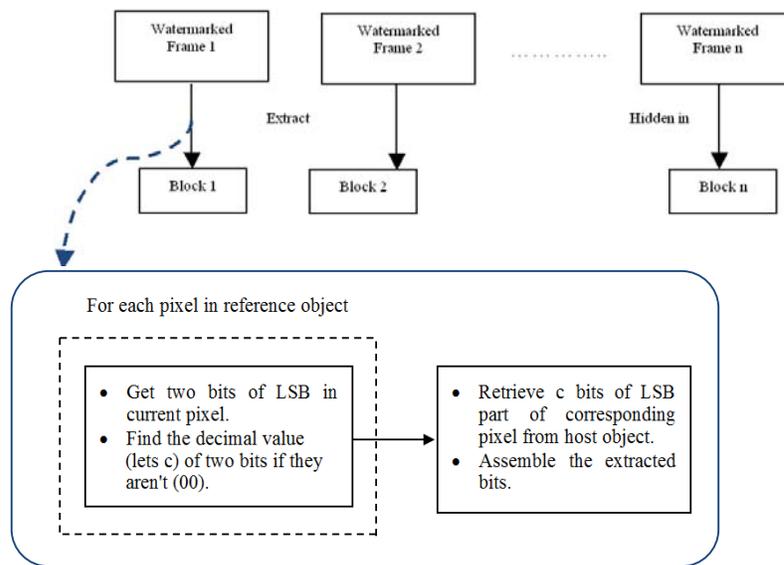


Fig. 5: Block diagram of a watermark's block extracting

Algorithm Name: Watermark Extraction.

Input: Watermarked Video file.

Output: Extracted Watermark.

Begin

Step 1: Separate watermarked video file to set of frames.
 Step 2: For each frame F from current frame to current frame + number of watermark's blocks
 Step 3: For each pixel in reference object while the block's bits don't be retrieved do
 Step 4: Check the 2LSB of current pixel that represents the counter c.
 Step 5: Retrieve c bits from the LSB part of the corresponding pixel of host object as:
 If c is 1 then get one bit-LSB
 Else If c is 2 then get two bit-LSB
 Else If c is 3 then get three bit-LSB
 Step 6: End // For each pixel
 Step 7: Assemble the retrieved bits from of frame F which represent a block's bits
 Step 8: End // For each frame
 Step 9: Assemble the retrieved blocks which represent a watermark's bits
 Step 10: Create BMP image file.
 Step 11: Convert each 8 bits from the total assembled bits to the corresponding color value.
 Step 12: For each three consecutive color values (three bands of RGB) do
 Step 13: Build a pixel of the watermark image and put it in data part of the created image file
 Step 14: End // For each three color values
 Step 15: Return the watermark image.
 End

Robustness against attacks: There are two attacks were applied to the watermarked video, they are frame dropping and frame swapping, the purpose of experiencing these attacks is that when the attacker does attacking and the receiver party or the owner of video don't know that.

The purpose of an attack is to make the video's owner retrieves false, incomplete information, or extracts a watermark which is not similar to the original watermark without knowing in which place of video's frames an attack was done. When frame dropping and frame swapping attacks were experienced on the frames of watermarked video, the video's owner or the receiver party can know the type and in which frames does an attack occur if it dropping or swapping the frames and he can retrieve the watermark properly, in addition to process what happened by the attack and reconstruct the dropped frames to get a video closer to being as the original video.

Frame dropping attack: Dropping was done by deletion frames from the watermarked video's frames, this causes that number of frames of attacked video that was watermarked are less than number of frames in original video. Since a block of watermark image was concealed in each frame, so that if the second party doesn't known which frames were dropped, the water mark will be extracted with missing blocks of dropped frames and the sequence of blocks will also be changed. This causes extracting wrong watermark.

To solve this state in frame dropping, the additional information that were embedded in each frame will be used

to know where the attack was and therefore the watermark's extraction will correctly be done according to the correct order of the blocks of watermark image.

The following algorithm shows how the blocks of watermark are extracted when there is frame dropping attack where F represents the number of current frame, B represents block's number that is stored in the current frame, P represents the number of watermark's repetition and K is the number of blocks of watermark image.

Algorithm Name: Watermark's Extraction with the Frame Dropping Attack.

Input: Attacked Video file.

Output: Watermark Image, Reconstructed Video File.

Begin

Step 1: Separate attacked video file to set of frames
 Step 2: For each frame apply the following equation to know which frames were dropped

$$Z = [F - (B + (P * k))]$$

 Step 3: If z equal to zero then
 Step 4: Check the next frame by the above equation
 Step 5: Else
 Step 5-1: Save the number of current frame
 Step 5-2: Change number of each frame from the current frame to the last frame
 Step 5-3: Reapply the equation to the current frame
 Step 6: End // If
 Step 7: Retrieve each missed block from another frame contains that block
 Step 8: Reconstruct each dropped frame from the average of its pre and post frames.
 End

Frame swapping attack: In this type of attacks an attacker does swapping in ordering of frames, in which the total number of frames hasn't been changed. This causes incorrect ordering in blocks of watermark but with the aiding of additional information which were concealed in each frame, the blocks of watermark can be extracted with correct sequence.

Frame swapping makes a frame with its contains but with the name of another one frame, this state alters in the ordering of blocks extraction and doesn't return the required watermark image. The following algorithm clarifies how the blocks of watermark are extracted when there is frame swapping attack.

Algorithm Name: Watermark's Extraction with the Frame Swapping Attack.

Input: Attacked Video file.

Output: Watermark Image, Reconstructed Video File.

Begin

Step 1: Separate attacked video file to set of frames
 Step 2: For each frame apply the following equation to know which frames were swapped:

$$Z = [F - (B + (P * k))]$$

 Step 3: If z equal to zero then
 Step 4: Check the next frame by the above equation
 Step 5: Else
 Step 5-1: Save the number of current frame
 Step 5-2: Save the number of block of current frame
 Step 5-3: Save the number of watermark's repetition of current frame
 Step 6: End // If
 Step 7: Depending on the information that were saved where the swap was done is known
 Step 8: Exchange with the names of swapped frames
 Step 9: Reconstruct the video.
 End

RESULTS AND DISCUSSION

The proposed system was applied with experimenting different watermark images, the watermark image is BMP color image (RGB). The movie that was used is with extension AVI, so that if any video with another extension, it must be translated into AVI file. Firstly separate the input video into set of frames, one of the experiments is indicated below by using the AVI video about movement of Chlorophyta under the microscope. Figure 6 shows samples of frames, while Figure 7 shows samples of watermark image that were hidden.

As mentioned in the section 4 that the watermark will be concealed in the most active object among all tracked objects, whereas the most active object was denoted by host object and the second most active object was denoted by reference object. Host object was utilized to embed in its area a block of data of watermark image, with different number of bits (0, 1, 2, or 3 bits) that will be hidden in each pixel of a specific area of host object. Reference object was utilized to embed in the corresponding pixel the number of bits that were hidden in a pixel of host object. Figure 8 illustrates samples of frame before and after watermark' block concealing.

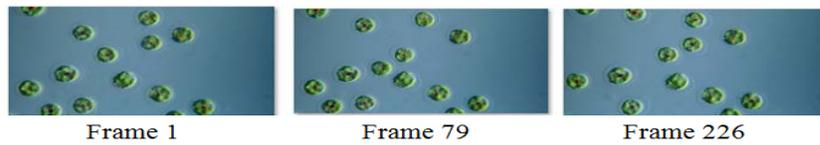


Fig. 6: Samples of frames of video



Fig. 7: Samples of watermark image

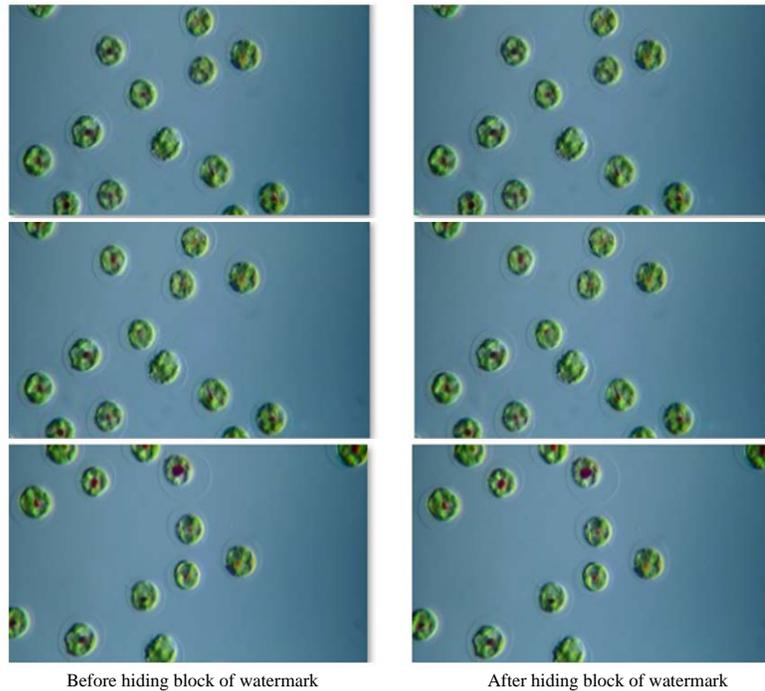


Fig. 8: Samples of frame before and after watermark' block concealing

Table 1: Extracted watermark with frame dropping attack

Extracted watermark image	Normalized Correlation (NC)
	0.8
	0.91
	1

Table 2: Extracted watermark with frame swapping attack

Extracted watermark image	Normalized Correlation (NC)
	1
	1
	1

In watermark extraction operation, reference object was depended to know the number of bits from the watermark's block that were embedded in host object by checking the least two bits in each pixel of reference object. These least two bits in each pixel represent as index that is very important in extraction of the watermark. After apply attacks of frame dropping, the block of watermark that was embedded in the dropped frame will be lost but by using the saved information, the dropped frames will be known and the block of watermark can be retrieved from another frame contains such block. Table 1 illustrates the extracted watermarks with the normalized correlation measure which was used to evaluate the similarity of the original watermark with the retrieved watermark.

While when apply frame swapping attack, any block never lost because it is founded but in another frame that was swapped with another frame, by using the additional information that were saved after watermark's block concealing in each frame, the entire watermark's blocks were extracted with complete similarity between retrieved and original watermarks. Table 2 shows the extracted watermarks with the normalized correlation measure.

CONCLUSION

To increase the powerful and the adeptness of the proposed hiding algorithm in this study, it doesn't depend on hiding the watermark in fixed location in the video's frames. In order to avoid the weakness of concealing the watermark in the same position through the frames, so that the adaptive algorithm of this study tends to embed each a block of watermark in different places within the frames. It depends on selecting two objects (host and reference) which are active in their motion through the video, whereas the location of hiding watermark is located within the object in a frame which is varied according to the motion of that object.

The algorithm also doesn't conceal fixed number of bits from watermark's block in LSB part of each pixel, instead of that, in each time the algorithm conceals varied number of bits from block of watermark in LSB part of each pixel of host object depending on the difference between the current pixel and its neighbors, with storing the number of hidden bits in two bits at LSB part in reference object.

The experimental results show a small modification in both object and reference objects, this doesn't cause perceptual degradation in frames of video due to the hiding operation using LSB, many pixels in the area of host and reference objects are modified whereas LSB modifies as maximum 3bits in the least significant part of the pixel. So that only area of hiding in both objects are changed in its pixels values (not all its pixels, just they are enough for hiding bits of watermark's block). Also, the experimental results indicates the samples of extracted watermark images with measuring the normalized correlation between extracted and original watermarks. The value of NC measure influenced by number of dropped frames and which are they, because it is probably dropping the frames that a certain block embedded in for many repetition of the watermark, so that in this case such block will be lost, this makes decreasing in NC value.

ACKNOWLEDGEMENTS

Researcher thanks and offers the gratitude to the information technology college for its support to the Postgraduates. Also, Researcher presents the thankfulness to the supervisor for her observations and encourage along the work.

REFERENCES

- Abinaya, M. and S. Elango, 2014. Video source tracking and copyright protection in video watermarking. *Int. J. Innovative Res. Sci. Eng. Technol. (IJIRSET.)*, 3: 13977-13986.
- Ali, I.H. and A.S.S. Murieb, 2015. Adaptive algorithm for watermark hiding in video objects. *Int. J. Digital Content Technol. Appl.*, 9: 9-17.
- Bhattacharya, S., T. Chattopadhyay and A. Pal, 2006. A survey on different video watermarking techniques and comparative analysis with reference to H 264-AVC. *Proceedings of the 2006 IEEE International Symposium on Consumer Electronics*, June 28-July 1, 2006, IEEE, Kolkata, India, ISBN:1-4244-0216-6, pp: 1-6.

- Bhaumik, A.K., M. Choi, R.J. Robles and M.O. Balitanas, 2009. Data hiding in video. *Int. J. Database Theory Appl.*, 2: 9-16.
- Chan, P.P.W., M.R. Lyu and R.T. Chin, 2004. Copyright protection on the web: A hybrid digital video watermarking scheme. *Proceedings of the 13th International World Wide Web Conference on Alternate Track Papers and Posters, May 17-22, 2004*, ACM, New York, USA., ISBN:1-58113-912-8, pp: 354-355.
- Chu, H.S., A. Batgerel and C.K. An, 2009. A semi-blind digital watermarking scheme based on the triplet of significant wavelet coefficients. *J. Electr. Eng. Technol.*, 4: 552-558.
- Essaouabi, A., F. Regragui and E. Ibnelhaj, 2009. A wavelet-based digital watermarking for video. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS.)*, 6: 29-33.
- Gupta, R., 2014. Information hiding and attacks: Review. *Int. J. Comput. Trends Technol. (IJCTT.)*, 10: 21-24.
- Gupta, R., S. Gupta and A. Singhal, 2014. Importance and techniques of information hiding: A review. *Int. J. Comput. Trends Technol. (IJCTT.)*, 9: 1-6.
- Israa, H.A., S. Safa, A. Murieb, 2016. Watermark hiding in video object based on complex shape trajectory. *Int. J. Inf. Proc. Manage. (IJIPM.)*, 7: 1-10.
- Katzenbeisser, S. and F.A.P. Petitcolas, 2000. Information hiding techniques for steganography and digital watermarking. *EDP Audit Control Security Newslett.*, 28: 1-2.
- Komal, P., S. Utareja and H. Gupta, 2013. A survey of information hiding techniques. *Int. J. Emerging Technol. Adv. Eng.*, 3: 347-350.
- Masoumi, M. and S. Amiri, 2012. A blind video watermarking scheme based on 3D discrete wavelet transform. *Int. J. Innovation Manage. Technol.*, 3: 487-490.
- Mauro, B., I. Cox, T. Kalker and H.J. Kim, 2005. *Digital Watermarking*. Springer, Berlin, Germany.
- Shojanazeri, H., W.A.W. Adnan and S.M.S. Ahmad, 2013. Video watermarking techniques for copyright protection and content authentication. *Int. J. Comput. Inf. Syst. Ind. Manage. Appl.*, 5: 652-660.
- Wayner, P., 2002. *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*. 2nd Edn., Morgan-Kaufmann, San Mateo, CA., pp: 81-128.