Comparison between Hiding in Corners Regions and Hiding in Regions between Corners by using Characteristic Regions of FAST Corner Detection

Dr.Abdulameer A. Karim **Ekhlas Falih Nasser**

ameer_aldelphi@yahoo.com ekhlas_uot1975@yahoo.com

Abstract

The invisible science of communication is called steganography. It employs various useful applications. Hiding of information change almost whole cover image for most techniques of steganography that perhaps affect negatively the visual quality of an image and raise the potential of hidden data losing after the potential attacks. This research offers a novel technique for steganography based on hiding between corners regions to solve this problem, which was hiding data in the robust regions of an image. The approach has been employed to discover the robust image regions between corners which are resulted by employing features from accelerated segment test (FAST) method. The outcomes displayed that the accuracy of hiding data between corners regions is higher for retrieving an embedded data and that the visual embedded image quality than embedded data into corners regions themselves.

Keywords: Information hiding, Steganography, FAST, LSB, Extracting.

مقارنه بين الأخفاء في مناطق الزوايا والمناطق بين الزاويا بأستخدام خصائص مناطق كاشف الزاؤيه السريع

أ.م. د.عبدالأميرعبدالله كريم **م.أخلاص فالح ناصر**

الجامعة التكنولوجية / قسم علوم الحاسوب

الخلاصه

يسمى علم الأتصال غير المرئي بالأخفاء فهو يستخدم في مختلف التطبيقات المفيدة. ان إخفاء المعلومات يغيير غالباً صورة الغلاف كلها في معظم تقنيات الأخفاء والتي ربما تؤثر سلبا على جودة الصورة بصرياً وترفع احتمالية فقدان البيانات المخفيه بعد الهجمات المحتمله. يعرض هذا

البحث تقنيه جديده للأخفاء بالأعتماد على الأخفاء بين مناطق الزوايا لحل هذه المشكله، والتي فيها يكون الأخفاء في المناطق القويه للصوره.الطريقه المستخدمه لأكتشاف المناطق القويه في الصوره بين الزاويا الناتجه وذلك باستخدام طريقة اختبار المقطع السريع للصفات (FAST) . أظهرت النتائج أن دقة إخفاء البيانات بين مناطق الزوايا يكون أعلى من ناحية استرجاع البيانات المخفيه وجودة الصورة المخفيه بصرياً مقارنة مع أخفاء البيانات في مناطق الزوايا نفسها.

1. Introduction

The internet and computers considered the major communication media in the recent era, which connect various world parts in one universal virtual world. People can interchange information readily and no longer distance for barrier communication. The communication security and safety for long-distance remains the issue. This is significant especially in the confidential data issue. The requirement to solve this problem has driven to steganography schemes development.

Steganography could be become a robust tool for security which can provide a supreme security level, especially when it is mixed with encryption [1].

Cryptography differs from steganography. The cryptography's goal is to secure communications through altering the data into a style that cannot understand by eavesdropper. On other hand, steganography's techniques attempt to hide whole message presence, where an observer does not realize that there is any message. In several cases, encrypted information that send may attract the attention but it will not attract any attention when sending invisible information. For insurance communication, cryptography is not the optimum solution but it is part of the solution only. To better protect information, both cryptography and steganography can be employed together. In this status, when steganography technique fails, it cannot be recovered the message; because a technique of cryptography is well employed [2]. It can measure a steganographic system performance using numerous properties such as

1) The data statistical undetectability is the important property which shows how difficulty for locating the hidden message existence.
2) The steganographic capacity is another measure which determines the maximum loading that can safely hidden in a task without making detectable objects statistically [3].
3) The robustness of steganographic system is the third measure which indicate to how perfectly the resists for hidden data elicitation.

Although all formats of digital file can be employed for steganography, but the most suitable formats that have a high redundancy degree. An object

excrescence bits refer to the bits that can be altered without readily alteration detection. This requirement can be satisfied by audio and image files [4]. The most formats that can be employed as carrier file are digital images such as bitmap images (BMP) because of their publicity on internet. For most of the image, information hiding alters almost all components of the cover for most current techniques of steganography in image, which may affect negatively the quality of image visually and increase the potential of data losing after the potential attacks. Adaptive steganography defines textural or quasi-textural regions for embedding data secretly. Adaptive steganography picks statistical features from an image before trying to embed the secret information in special image regions. The statistics can build a rule where to make the modification [5].

The technique of characteristic identification must be robust to survive after communication errors or potential attacks. Surveying the literature [5], Li et al. employed a characteristic region, using scale invariant features transform (SIFT) for obtaining synchronization of an image watermark for the purposes of copyright protection. Their scheme can be synchronized a high capacity hiding of information and generalized robustness in watermark.

The present paper focuses on the adaptive steganography to hide the secret information in the digital video files. The approach has been employed to detect the regions in video frames which are robust based on FAST corner detection.

2. Classical steganography method using Least Significant Bit Substitution

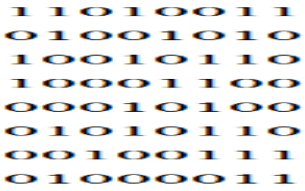
LSB steganography employs the least significant bits from the cover data for message hiding. Substitution in LSB is the simplest technique of LSB techniques.

Substitution in LSB technique flips the last bit of all values of data for reflecting the message, that desire to hide. Suppose a gray scale image that can be stored a value of gray scale as a byte for every pixel in an image.

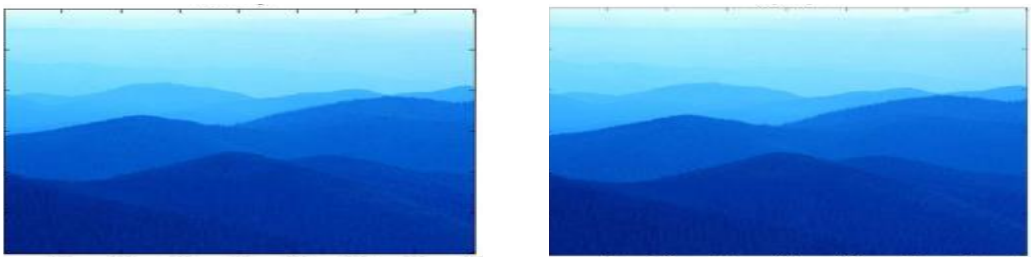
Assume eight pixels can be taken from the ethnic image as illustrated in the following:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

For embedding the binary value of letter C (10000011), it can be substituted the LSBs of eight pixels for resultant the following values of gray scale:



Only half the technique of LSB requires changing. The variance between the cover and the stego images will be difficult to notice by the human eye [6]. Figure ((1) (a), (b)) that display a cover and a stego images respectively, there is no visual difference between these images.



(a) **(b)**

Figure (1): Bitmap images (a) Cover Image (b) Stego Image

3. Proposed Methodology for Steganography Synchronization Based on FAST Corner Detector

Synchronization of steganography means that processes of data embedding and elicitation can be performed in the same area. Synchronization of steganography can be obtained in this paper through the characteristic areas based on features from accelerated segment test (FAST) corner detection technique. Data is embedding in particular regions of an image based on their characteristics. The same characteristics must be employed to identify the embedded areas exactly to start the elicitation process.

FAST corner detector can be employed for synchronization of steganography in present task into two suggested schemes. Then, a comparison between the suggested schemes is presented.

3.1 Algorithm Description

The synchronization algorithm of steganography depends on two stages: robust corners (key-points) are eliciting from a video frames and hiding data in these key-points. The key-points or corners of an image are robust if they are resisting to the operations of image processing, such as rotation and scaling. The robust areas are detecting when the image pass into various attacks. The opinion of choosing those corners for hiding of information secretly is to ensure that the positions of the corners in which the data is hidden can be determined without a map for embedding.

Moreover, the corners in which the data can be embedded are not fixed and highly dependent on image characteristics that employed as a cover.
Also, selecting a few corners for data hiding will reduce the deformation of stego-image. For the stage of data hiding, the information is embedded secretly using a FAST corner detector.

3.2 Extracting Key-points using FAST

The standard computers have fast processing power enough for corner extraction at the rate of video. However, running traditional algorithm for corner detection such as the detector by Harris algorithm and performing heavy tasks make impossible computation on one processor. At the introduction of modern algorithms like FAST (Features from Accelerated Segment Test) [7], elicitation the feature consider great increase for the performance of computer vision applications in real-time. A circular region's center can be used for defining neighboring brighter and darker pixels.
FAST algorithm doesn't evaluate the whole circle's region, but only the pixels on discretization circle for segment's characterization. FAST uses a Bresenhams algorithm for circle drawing with diameter of 3.4 pixels for trial mask. Trial 16 pixels compared to the nucleus's value for a complete accelerated segment. The criterion of corner should be more relaxed to block this broad trial. A pixel's criteria must be a corner based on the accelerated segment test (AST) which there must exist at least S pixels that have more brilliant circle connection or darker than a threshold designer by the center pixel value. Other values of 16 pixels are disregarded. So the value of S can be used to determine the detected corner at maximum angle [8]. Figure (2) shows an example of the characteristic regions generated on Tracery's image.

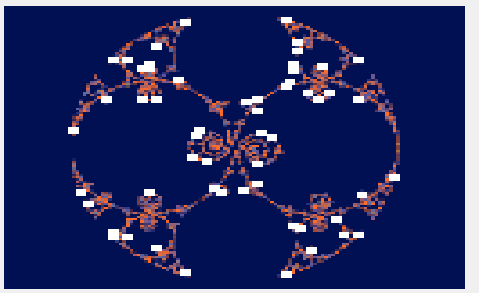


Figure (2): Characteristic corners extracted from Tracery's image

The steps of FAST algorithm can exposure below:

1. From an image, chose a pixel **p**". $\mathbf{I_P}$ represent pixel's intensity. This pixel can be specified as a point of interest or not as illustrated in figure (3).

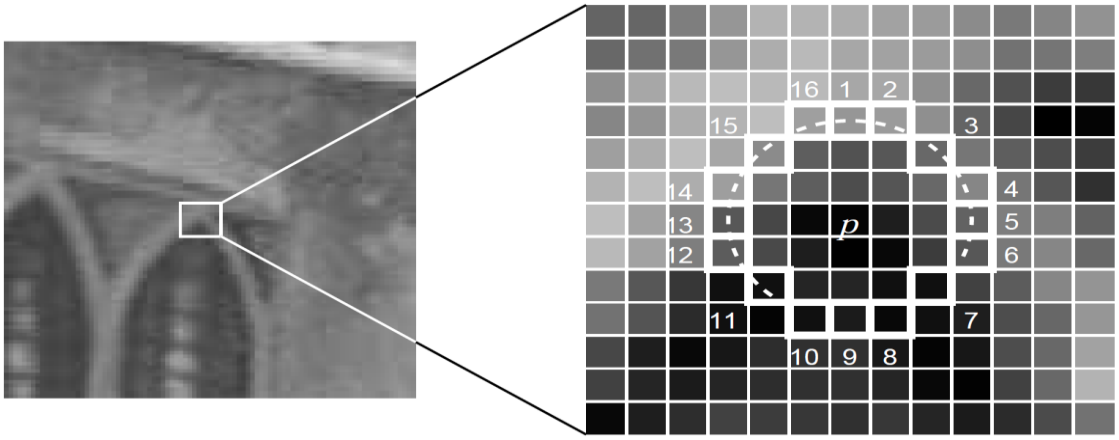


Figure (3): Image display the point of interest under a test and the circle of 16 pixels

2. Choose **thr** that represents the value of threshold intensity**.**
3. Assume periphery a pixel **p** the circle of 16 pixels. (a Bresenham circle [4] of radius 3.)
4. Need "**N**" exposure nearby pixels far from the 16 pixels, either below or above $\mathbf{I_P}$ by **thr** value, if the pixel wants to discover as a point of interest.
5. First match 1, 5, 9 and 13 of the circle pixels' intensity with $\mathbf{I_P}$ to make an algorithm fast. From figure (3), at least three of these four pixels should accept the norm of the threshold for this it subsist an interest point.
6. **P** is not an interest point (corner) if at least three values of - $\mathbf{I_1}$,$\mathbf{I_5}$,$\mathbf{I_9}$ $\mathbf{I_{13}}$ are not below or above $\mathbf{I_P}$ **+ thr**. For this a pixel **p** can be rejected as a potential point of interest. Else if three pixels at least are up or down $\mathbf{I_p}$ **+ thr**, for whole **16** pixels seek and check if 12 neighboring pixels drop in the norm [8].
7. A same procedure can iterate for whole image's pixels.

3.3.1 Suggested Schemes

After extracting numerous invariant corners for steganography synchronization on video frames, the data can be embedded secretly into the specific corners regions or in the regions between corners based on least significant bits (LSB) of those corners as illustrated in figure (4).

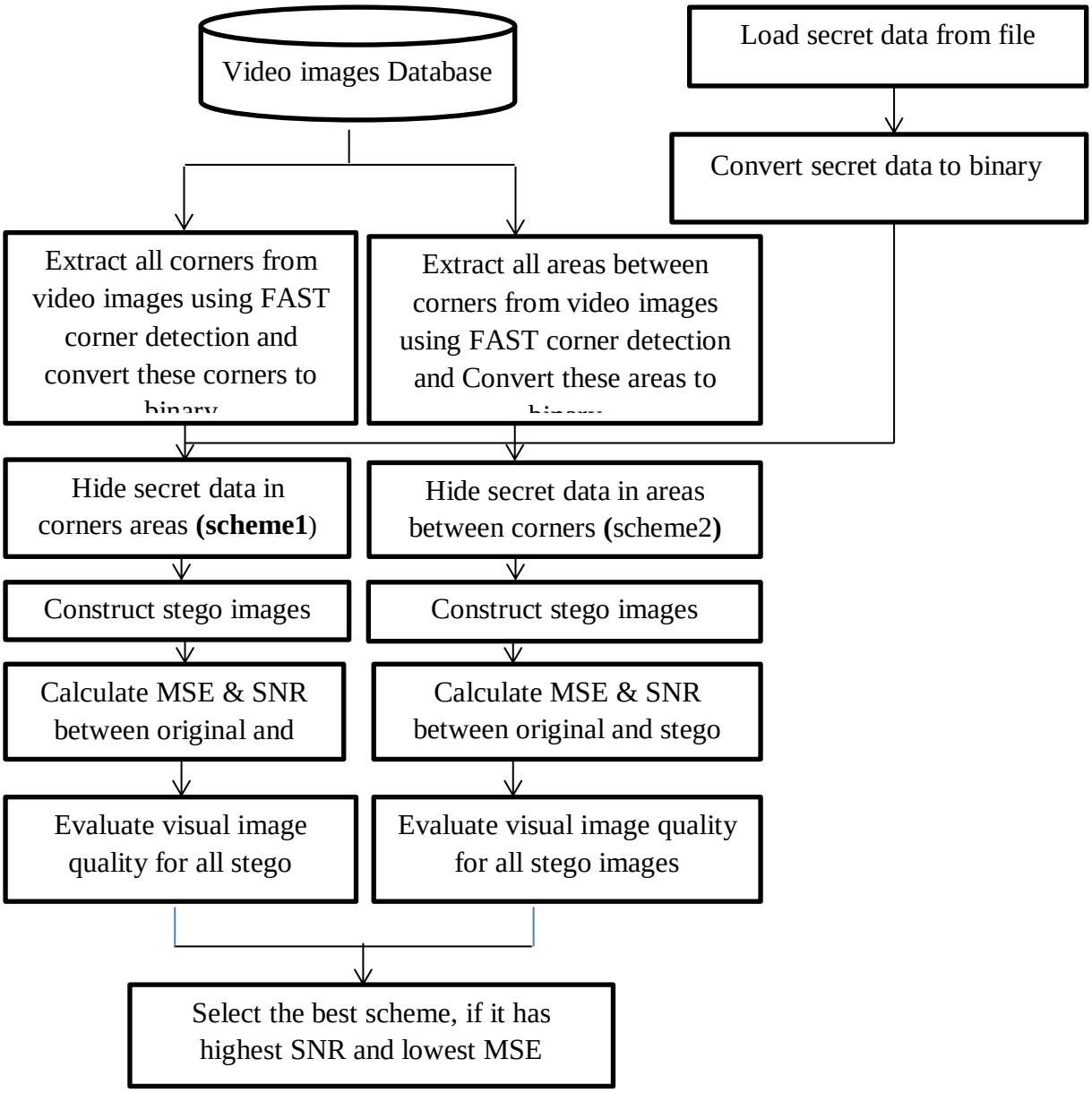


Figure (4): Block Diagram of the Proposed Schemes

The suggested system based on two schemes for hiding and extracting the data

I. Data Embedding and Extracting in Corners Themselves Scheme(1)

In the embedding step, all corners are chosen from the cover image, encode one secret bit in the LSB of each corner, and then construct a video for transfer.

In the extracting process, the LSB of all corners in video frames are calculated and lined up to reconstruct the message.

II. Data Embedding and Extracting in the Areas between the Corners Scheme(2)

In the embedding step, all areas between the corners are chosen from the cover image, encode one secret bit in the LSB of each area, and then construct a video for transfer.

In the extracting process, the LSB of all areas between the corners are calculated and lined up to reconstruct the message.

III. Evaluation of the Suggested System

For quality estimation for the suggested schemes performance, two measurements for quality were employed; signal to noise ratio (SNR) and mean squared error (MSE) where SNR refer to the amount of signal to distortion ratio after hiding process [9].

To calculate the SNR between two images the following equation can be used:-

$$SNR = \sum_{x,y} P_{x,y}^2 * \sum_{x,y} (P_{x,y} - P'_{x,y})^2 \qquad \dots (1)$$

For counting the MSE between the ethnic and suspicious images, the difference of pixel color in the two images must be taken [9].

$$MSE = \frac{1}{N * M} \sum_{x,y} (P_{x,y} - P'_{x,y})^2 \qquad \dots (2)$$

where $P_{x,y}$:-The values of pixel in location x and y of the ethnic image.
$P`_{x,y}$:-The values of pixel in location x and y of the stego image.
N and M are the width and height of an image

4. Proposed Algorithms for Schemes

The suggested method consists from two schemes for hiding and extracting the secret messages. In the first scheme, the hiding process can be implemented inside corners regions but in the second scheme, the hiding process can be implemented inside regions between corners. Algorithm (1) can be employed for hiding secret messages inside corners regions. Algorithm (2) can be employed for extracting secret messages from corners regions. Algorithm (3) can be employed for hiding secret messages inside regions between corners. Algorithm (4) can be employed for extracting secret messages from regions between corners.

The algorithms of the proposed schemes are illustrated as:

Algorithm (1): Embedding Process on Corners Regions themselves

Input: - load AVI video and extract it frames, load secret text. Output:- Video of stego frames.
Step1:- Apply FAST corner detector for all video frames to extract the corners. Step2:-convert the pixels at these corners and secret text to binary. Step3:- set the variables 3.1) Set N to the number of corners in the cover, set M to length of binary message. 3.2) Set i to 1, set j to 1, set sign to the end of secret message. Step4:- if M>N then return "cover not suitable for hiding", stop. Step5:- while i <N and j<=M do LSB(corner(i))=message(j) i=i+1 j=j+1 end while Step 6:- construct a video form stego frames. Step 7:-end

Algorithm (2): Extraction Process from Corners Regions

Input: - video of stego images. Output: - secret message.
Step1:- extract stego images from the video. Step2:- Apply FAST corner detector for all video images to obtain the corners. Step3:- convert the pixels at these corners to binary. Step4:- Set i to 1 set j to 1. Step5:-while secret(j)<> sign do Extract_ message(j) = LSB (corner(i)) i=i+8 j=j+1 end while Step 6:- lined up message (j) to reconstruct the secret message. Step7: end.

Algorithm (3): Embedding Process on Regions between Corners

Input: - load AVI video and extract it frames, load secret text. Output:- Video of stego frames.
Step1:- Apply FAST corner detector for all video frames to extract the corners, and extract all areas between corners Step2:-convert the pixels at the areas between corners and secret text to binary. Step3:- set the variables 3.1) Set N to the number of areas between corners in the cover, set M to length of binary message. 3.2) Set i to 1, set j to 1, set sign to the end of secret message. Step4:- if M>N then return "cover not suitable for hiding", stop. Step5:- while i <N and j<=M do LSB (area between corner(i))=message(j) i=i+1

```
        j=j+1
      end while
Step 6:- construct a video form stego frames.
Step 7:-end
```

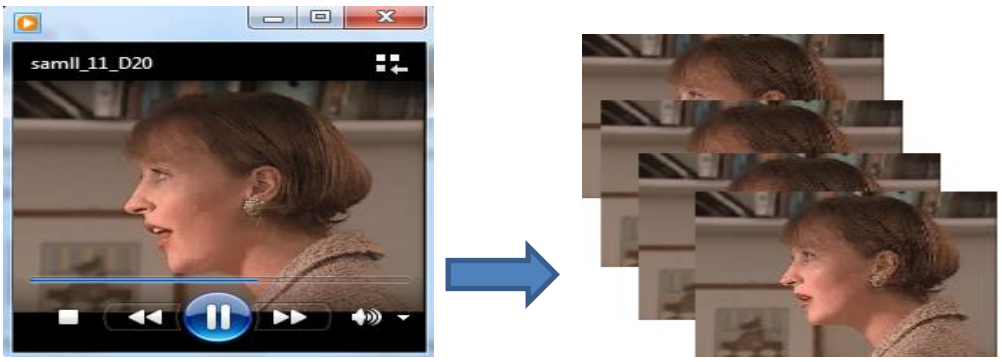
Algorithm (4): Extraction Process from Regions between Corners

```
Input: - video of stego images.
Output: - secret message.
Step1:- extract stego images from the video.
Step2:- Apply FAST corner detector for all video images to obtain the corners and extract all areas between corners.
Step3:- convert the pixels at these areas to binary.
Step4:- Set i to 1 set j to 1.
Step5:-while secret(j)<> sign do
       Extract_ message(j)=  LSB (area between corner(i))
        i=i+1
       j=j+1
      end while
Step 6:- lined up message (j) to reconstruct the secret message.
Step7: end.
```

5. Experimental Results

The outcomes of suggested method are offered and discussed at this part. The suggested method is executed in C#. Three types of databases like Women Conversation, Crocus, and Planets from video frames are employed for evaluation the suggested mode. Database images are bitmap (BMP) colored, and with size 320 × 240 pixels. The suggested method consists from multiple steps:-

1) The process of loading a video file onto the form of the project can be implemented in the first step as illustrated in figure (5) (a), figure (7) (a), and figure (9) (a).
2) In the second step ,the cover frames can be extracted from video file as illustrated in figure (5) (b), figure (7) (b), and figure (9) (b).



a) **b)**

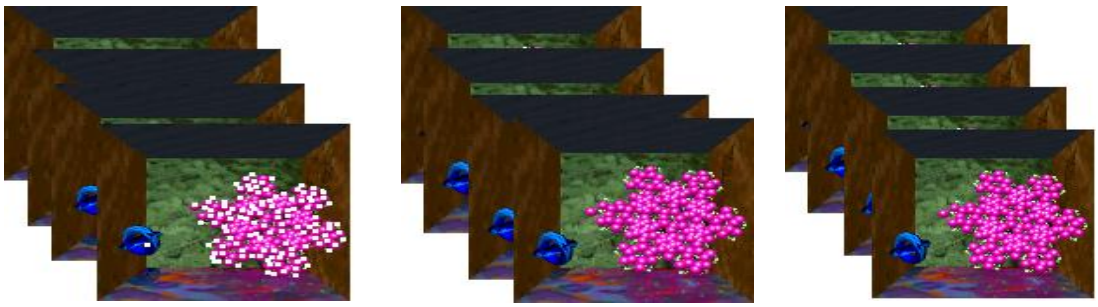
Figure (5): a) Input Conversation Video b) Extract Cover Frames

3) Corners can be detected in the third step using FAST corner detector as illustrated in figure (6) (a), figure (8) (a), and figure (10) (a).
4) In the forth step,hiding process can be implemented inside the corners regions as illustrated in figure (6) (b), figure (8) (b), and figure (10) (b).
5) In the fifth step,hiding process can be implemented inside the regions between corners as illustrated in figure (6) (c), figure (8) (c), and figure (10) (c).

a) **b)** **c)**

Figure (6): Video Frames a) Detect Corners on Video Frames b) Stego Frames which are resulted from Hiding Data inside Corners Regions c) Stego Frames which are resulted from Hiding inside Regions between Corners.

Figure (7): a) Input Crocus Video **b) Extract Cover Frames**



a) **b)** **c)**

Figure (8): Video Frames a) Detect Corners on Video Frames b) Stego Frames which are resulted from Hiding Data inside Corners Regions c) Stego Frames which are resulted from Hiding inside Regions between Corners.

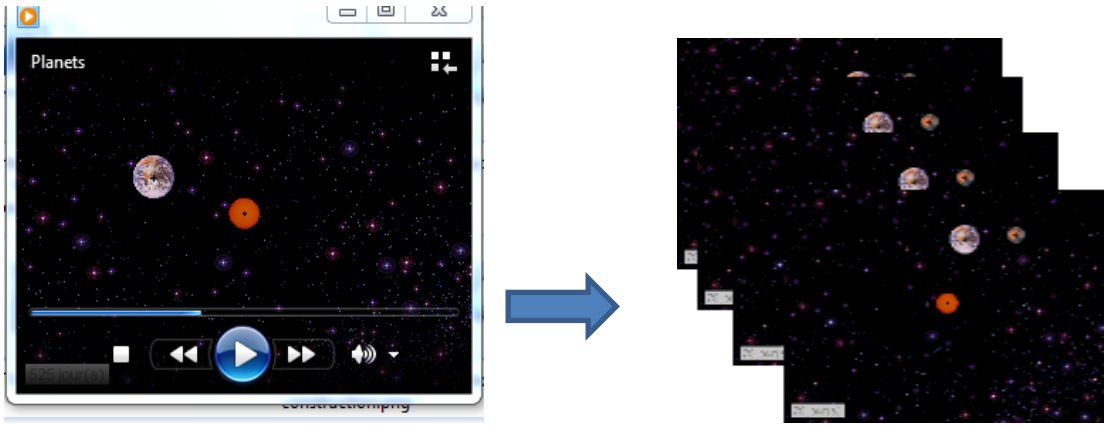
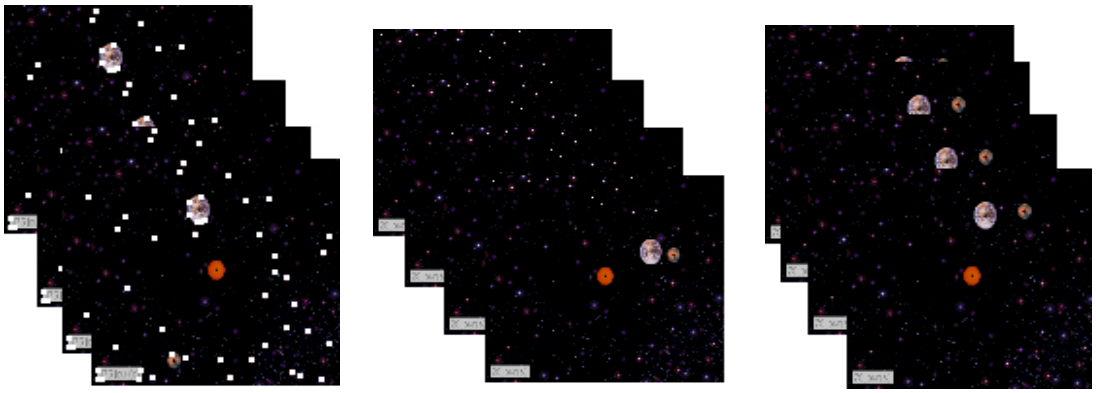


Figure (9): a) Input Planets Video **b) Extract Cover Frames**



a) **b)** **c)**

Figure (10): Video Frames a) Detect Corners on Video Frames b) Stego Frames which are resulted from Hiding Data inside Corners Regions c) Stego Frames which are resulted from Hiding inside Regions between Corners.

Evaluation of the hiding process depends on two measures as mentioned in Eq.(1) and Eq.(2).

The distortion rate caused by the hiding process can be illustrated in table (1) on the red, green and blue bands. The values of MSE for red, green and blue are increased and SNR are decreased when the hiding process was implemented inside corners regions. On other hand, the values of MSE for red, green and blue are decreased and SNR are increased when the hiding process was implemented inside regions between corners.

Table (1) shows the comparison outcomes based on the effect of concealment on the third video image

Method name	Object name	MSE(Red)	MSE(Green)	MSE(Blue)	SNR(Red)	SNR(Green)	SNR(Blue)
Hide inside Corners	Women Conversation	12.87487	18.36791	20.72597	119	322	497
	Crocus	7.71564	5.82654	9.83545	2118	1122	6381
	Planets	18.45727	22.46124	14.88128	52	28	56
Hide inside Areas between Corners	Women Conversation	0.00348	0.00402	0.00384	444035	226699	373752
	Crocus	0.00415	0.00463	0.00384	395640	802608	287141
	Planets	0.00378	0.00323	0.00348	255558	201363	243129

6. Conclusion

This paper aims to compare between hiding in corners regions and hiding in regions between corners in steganography synchronization on video frames. The corners were detected using FAST corner detection algorithm. Two schemes have been employed on the same test frames. In the first scheme, the secret data can be hidden in coroners regions and in the second scheme; the secret data can be hidden in regions between coroners. The experimental outcomes in table (1) demonstrate that the comparison between these schemes in term of distortion rate that have negative effect on the visual image quality. The values of MSE for red, green and blue are increased and SNR are decreased when the hiding process was implemented inside corners regions. On other hand, the values of MSE for red, green and blue are decreased and SNR are increased when the hiding process was implemented inside regions between corners.

The visual quality of an image is still high as the highest values of SNR and lowest values of MSE, when it was applied hiding process in the regions between corners. It can conclude that the hiding process in regions between corners can be given best visual quality than hiding in corners regions.

References

[1] Halim S.A. and Sani M.F.A., "Embedding Using Spread Spectrum Image Steganography With Gf (2m)", in Production of the 6th IMT-GT Conference on Mathematics, Statistics and its Applications (ICMSA), University Tunku Abdul Rahman, Malaysia, pp. 659 - 666, Nov. 3-4 2010.

[2] EL-Emam N.N., "Hiding A Large Amount Of Data With High Security Using Steganography Algorithm", Journal of Computer Science, Vol. 3, No. 4, pp. 223-232, 2007.

[3] Cox I. J., Bloom M.L., Fridrich J.A., and Kalkert T., "Digital watermarking and steganography", 2nd ed., Morgan Kaufman Publishers, USA, 2008.

[4] Cheddad A., Condell J., Curran K., and Kevitt M., "Digital image steganography: Survey and analysis of current methods", Signal Processing J. Vol. 90, pp. 727–752, No. 3, 2010.

[5] Nagham Hamid, R. Badlishah Ahmad, and Osamah M. Al-Qershi," A Comparison between Using SIFT and SURF fo**r** Characteristic Region Based Image Steganography ",School of Communication and Computer Engineering, University of Malaysia Perlis (UniMAP), IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 3, May 2012.

[6] Vijay Kumar Sharma ,Vishal Shrivastava," A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection", M. Tech. Scholar, Arya college of Engineering & IT , Jaipur , Rajasthan (India), Journal of Theoretical and Applied Information Technology , Vol. 36 No.1**,** 15th February 2012.

[7] Jasmine Anitha J. Ȧ and Deepa S. M. Ȧ, "Tracking and Recognition of Objects using SURF Descriptor and Harris Corner Detection", ȦNehru Institute of Engineering and Technology(Anna University) ,Coimbatore, India, Vol.4, No.2, 2014

[8] Edward Rosten, Reid Porter and Tom Drummond, "FASTER and better: A machine learning approach to corner detection" , in IEEE Trans. Pattern Analysis and Machine Intelligence, Vol.32, pp. 105-119,2010.

[9] Himanshu Gupta, Prof. Ritesh Kumar, and Dr. Soni Changlani," Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", Lakshmi Narain College of Technology & Science, Bhopal, Madhya Pradesh International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com ,ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June 2013.