Journal of Engineering and Applied Sciences 14 (6): 1999-2006, 2019
ISSN: 1816-949X

Hiding Text in AVI Video File by Method of Least Significant Bit

Wessam Lahmod Nados and Nada A. Rasheed
University of Babylon, Hillah, Iraq

Abstract: This research aims to accomplish the process of hiding text file within the video file extension (AVI). In this research, a new steganography technique was proposed. First stage is dividing the film video into series frames (still images file extension BMP) and then determining who will be the hiden in the film the video and this will be the site of hiding is not at all the film clips but in sections that represent different scenes in the film that have been drawn from a series of successive sections in the film. As for the text file we want to hide shall be transferred to ASCII text and then stored at the sites that have been identified to hide and sites which represent the framework of scenes in the film by using the method of Least Significant Bit (LSB). The algorithm was tested several times and the results achieved demonstrate this approach is promising and is able to hid text in AVI video file accurately a variety of loads.

Key words: Steganography, least significant bits, AVI video file, text Hiding, framework , approach

INTRODUCTION

The world lives a revolution of science and technology and becomes easy to provide information required to search for methods of a good face many dangers and challenges on the security level of increased demand for security of information and protection with a shortage of the number of institutions and increase the amount of information in all branches of knowledge is different as well as the need to take advantage of technical developments in the field of information security, there are a number of intruders (hackers) for information trying to get to everything we must protect the information even for those of being able to accessible. Steganography deals with data to be sent (messages may be texts or images) within the data sent (preferably pictures to be of type bmp or audio or video files, so as to contain the amount of sufficient data which enables the programmer hide data within). Steganography differs from cryptography in that cryptography works on hiding the message content while steganography works on hiding the existence of another file in the message (Karasik and Smilansky, 2011). As for how this technology is to take advantage of the bits not important or those that are difficult to be discovered in the case was altered, contained within the image file or audio or video and used to hide the embedded message. What distinguishes this type of hidden messages is that they reach their destination completely confidential, unlike encrypted messages which although can never be deciphered without a key encryption, they can be identified as a message encrypted (Piccoli *et al*., 2015). Steganography technique aims to hide evidence in other data in a manner that does not lead to affect the latter, so that does not raise any suspicion or doubt that leads to uncovering the truth and purpose of the hiding that this is likely the attacker does not know of the existence of this data and thus are protected from reading or modification or destruction by the attacker (Gallagher, 2012). This means that steganography is not part of the encryption and there is a large difference between the two, for example, cryptography leaves a clear effect in the parameters of messages sent and does not require compromise and secondly to hide the data, It could be argued that the encryption is defined the face change the sender of the text in one of the many encryption algorithms. To make it difficult to understand after encrypted depends only on the sender and the reciever while science requires steganography the second compromise is hidden within the data does not require changing the parameters of data sent (Rousopoulos *et al*., 2011). Also, makes this technique different from the encryption in the encryption knows the attacker the existence of these data, may be able to access them but they cannot be read until after the break the code but able to remove them if in doubt. Does not harm the integration of flags together in the same work and certainly will add strength and durability will apply a encryption algorithms on the data to be sent first, then apply one of the algorithms steganography in my data will be sent far from first discovered and are difficult to decrypt that was detected Its existence. And this means that the data to be sent, called the coded data (Encoded) in case the application of the art encryption, while it is called data (hidden) in the case of application of

Corresponding Author: Wessam Lahmod Nados, University of Babylon, Hillah, Iraq

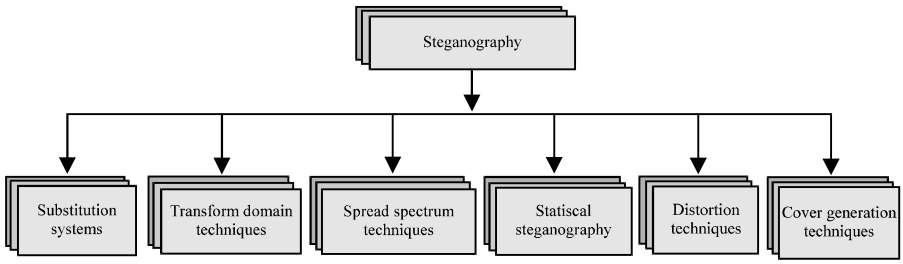


Fig. 1: Classification techniques of steganography

the steganography (Makridis and Papamarkos, 2010). As shown in Fig. 1 there are several methods used for the classification of systems of steganography of the mismatch depends on the type of cover used in secret communications and other support to make hanges (amendments) in the cap of steganography used in the process (Katzenbeisser and Petitcolas, 2000). The current paper aims to hide specific text within the video which included the proposed system implementation methods to hide different parts and each method has its own set of conditions that depend on them. The use of encryption with some ways to add another layer of protection to the hidden text (Richter *et al*., 2011) and we used the way the algorithm to decide at least the importance of hiding one method of concealment. Some processors has been made on the image containing hidden text, hidden text retrieval inside (Oxholm and Nishino, 2013; Shin *et al*., 2012; Stanco *et al*., 2011).

MATERIALS AND METHODS

Proposed system: In order to solve the stated problem, certain suitable model was proposed and built. The proposed system was implemented in many steps. It also, made use of all the available, modified and suggested tools and techniques. Figure 2a, b show the proposed system steps (Haralick *et al*., 1973). The proposed technique takes eight bits of secret data at a time and conceal them in LSB of RGB (Red, Green and Blue) pixel value of the carrier frames in 3, 3, 2 order, respectively. Such that out of 08 bits of message (06) bits are inserted in R and G pixel and remaining (02) bits are inserted in B pixel. The detailed technique has been depicted in Fig. 3. This distribution pattern is taken because the chromatic influence of blue to the human eye is more that red and green pixel. Thus, the quality of the video is not sacrificed but we could increase the payload (Makridis and Daras, 2012; Nados *et al*., 2014). Also, this small variation in colures in the video image would be very difficult for the

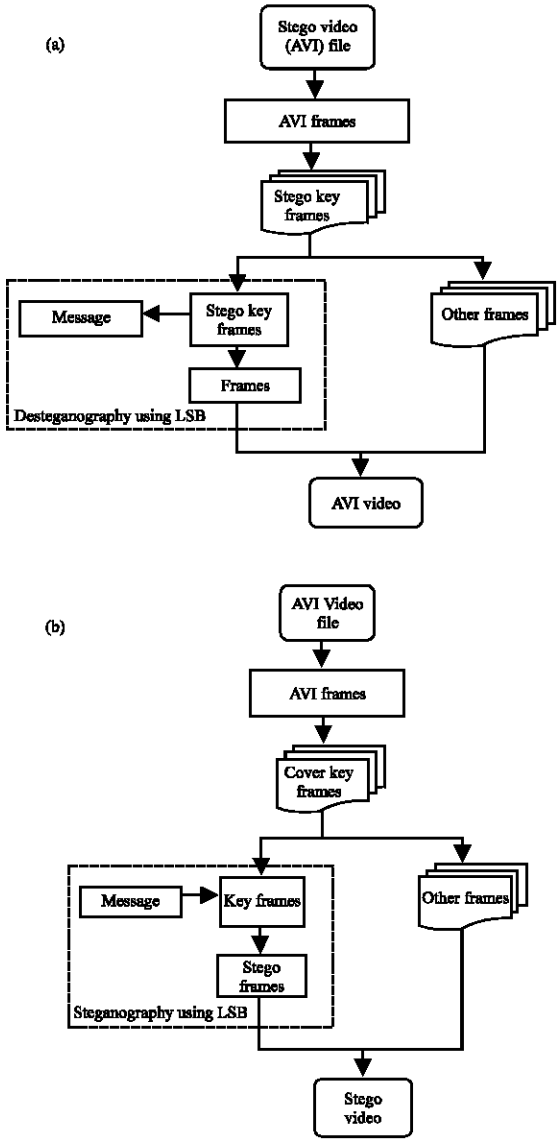


Fig. 2: Block diagram of LSB video steganography technique: a) Encodin and b) Decoding

human eye to detect. The bits are distributed randomly during fabrication which increases the robustness of the

technique compared to other LSB based techniques. After concealing data in multiple key frames of the carrier video, key frames are then grouped together to form a stego video which is now an embedded video to be used as a normal sequence of streaming. The intended user follows the reverse steps to decode the secret data. During decoding the setgo video is again broken into frames after reading the header. Information the extracted stream of the secret information is used to authenticate the video.

Algorithm 1; Algorithm of encoding:

Step 1: Inputing cover video file or stream
Step 2: Reading required information of the cover video
Step 3: Breaking the video into frames
Step 4: Extracting key frames (new scene) from sequence frames
Step 5: Selecting the (key frame +1) to hide text inside these frame
Step 6: Finding 4 LSB bits of each RGB pixels of the cover frame
Step 7: Obtaining the position for embedding the secret data
Step 8: Embedding the eight bits of the secret data into 4 bits of LSB of RGB pixels of the cover frame in the order of 3, 3 and 2 respectively using the position obtained from step 6
Step 9: Repeating step 5-8 for all key frames
Step 10: Constructing the video from all encoded frames

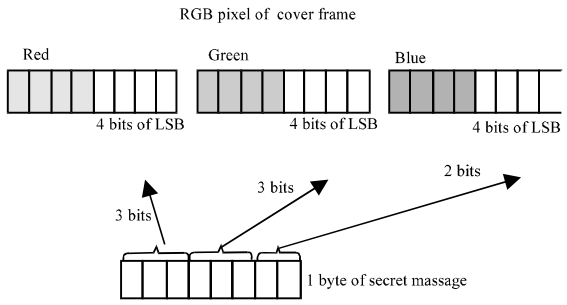


Fig. 3: Proposed LSB embedding technique, shows secret data embedded in 4 bits of LSB in 3, 3, 2 order in corresponding RGB pixels of the carrier frame

Algorithm 2; Algorithm of decoding:

Step 1: Inputing stego video file or stream
Step 2: Reading required information from the stego video
Step 3: Breaking the video into frames
Step 4: Finding 4 LSB bits of each RGB pixels of the stego frame
Step 5: Obtaining the position of embedded bits of the secret data
Step 6: Retrieving the bits using these positions in the order of 3, 3 and 2 respectively
Step 7: Reconstructing the secret information
Step 8: Regenerating video frames

RESULTS AND DISCUSSION

Experimental setup: This study includes the main steps of system running and the conclusion for our process. Therefore, the main components of the system are.

Main window of system: The main window contains the main component of hiding system. Also include some buttons for easy access to the system's function, so, Fig. 4 this process.

Main steps of running in the system

Step1: Clicking load movie button screen browser will be open. Then select the video and cutting the video into frames, the results as shown in Fig. 5a, b.

Step 2: Separate frames into scenes. The following Fig. 6 this process.

Step 3: Storage frames resulting from cutting the video after the presentation of the three main colors RGB, Fig. 7 the process.

Step 4: Storage scenes before and after the hiding. The following Fig. 8 this process.

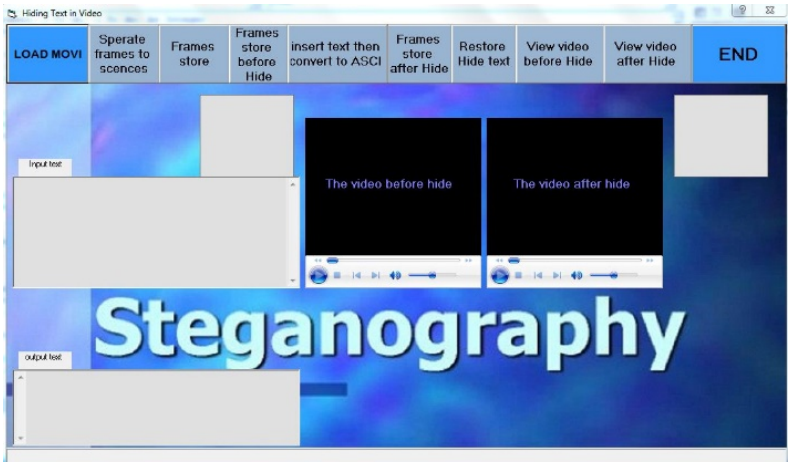
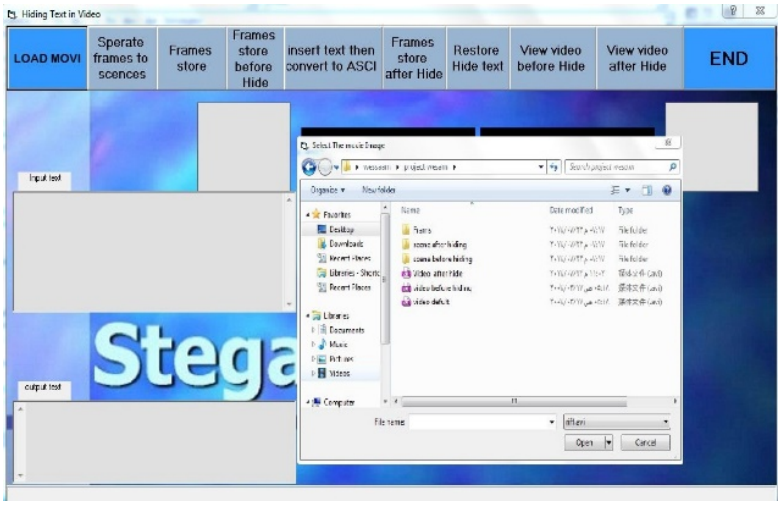


Fig. 4: User interface of hiding system

(a)



(b)

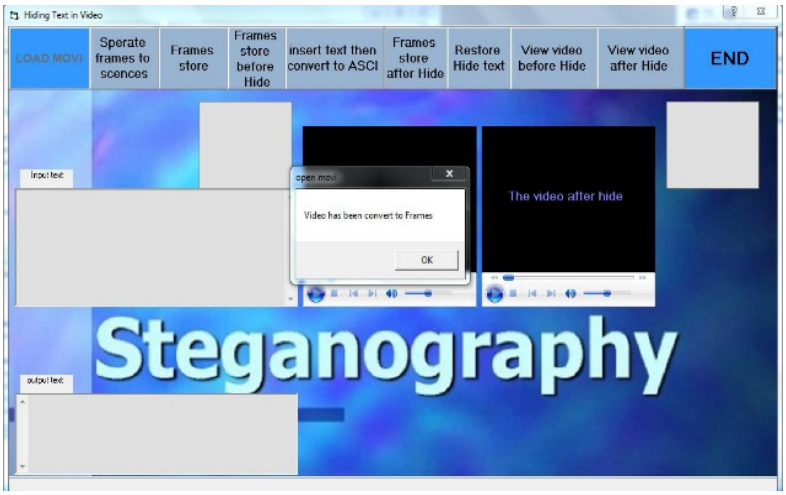


Fig. 5: a) Load movi and b) Convert the movi into frames

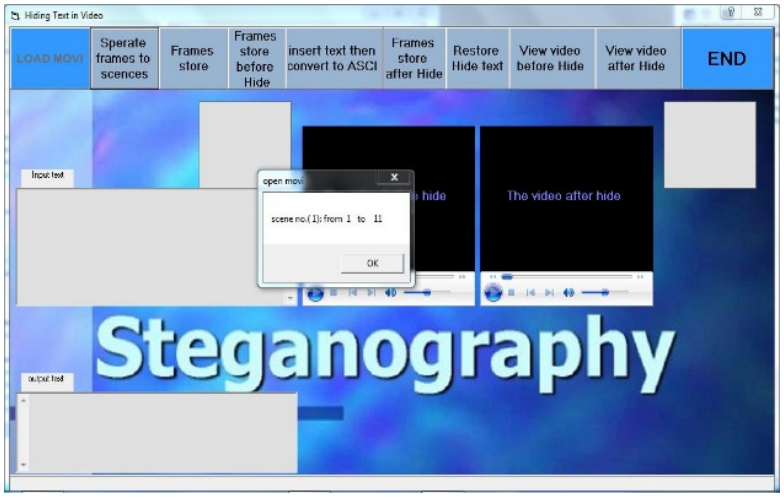


Fig. 6: Separate frames into scenes

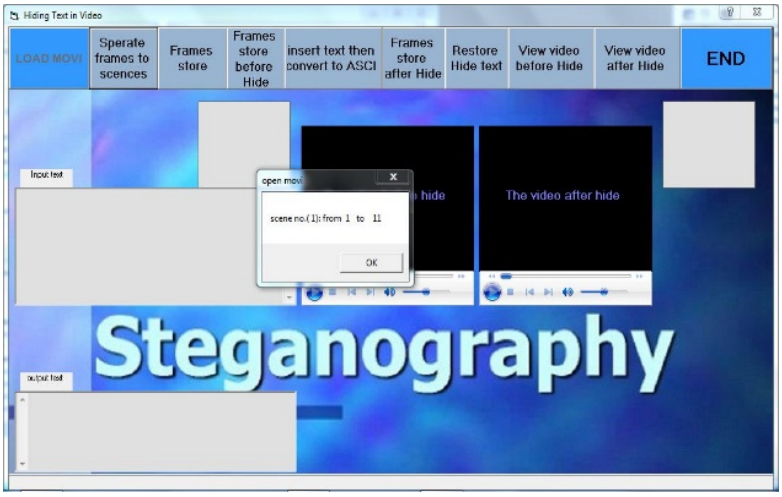


Fig. 7: Storage frames result

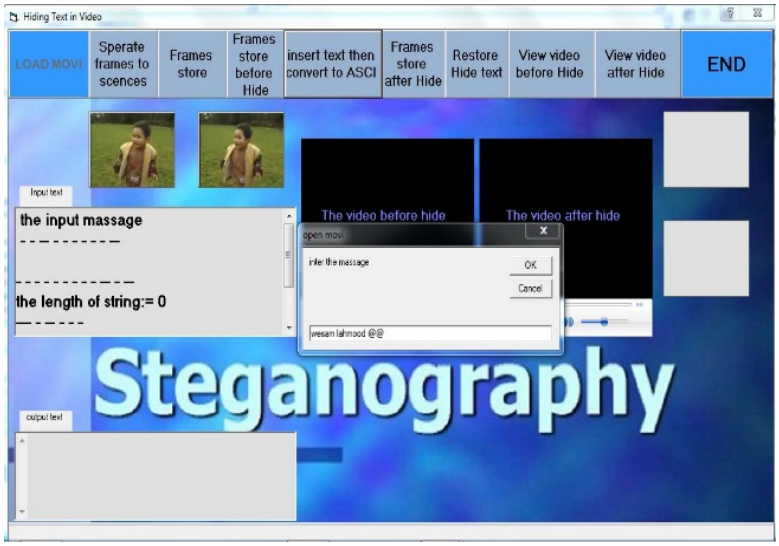


Fig. 8: Storage scenes before and after the hiding

Step 5: Hiding process applied to several texts in English (both large and small formulas) or Arabic or any other symbol. Where text is entered manually and calculates the number of characters entered and took each character ASCII. The following figure shows the form that contains the texts of English and Arabic were randomized to hide inside a video file. Figure 9 this process.

Also, a person cannot distinguish the existence of the text within the image (Frame) video and the following forms (1 and 2) show 53 Still Image Frame is made of the video file (which represents the movement of the child) are arranged horizontally according to the sequence displayed before the process of hiding after hiding. As shown in Fig. 10.

Two previous figures showed that there was no apparent difference with the naked eye by a process of hiding and after the process hiding. It is no secret that the movement of the video file will be the biggest obstacle to distinguish any difference, although, not his appearance which gives greater security for the transfer of hidden data (Fig. 11-13).

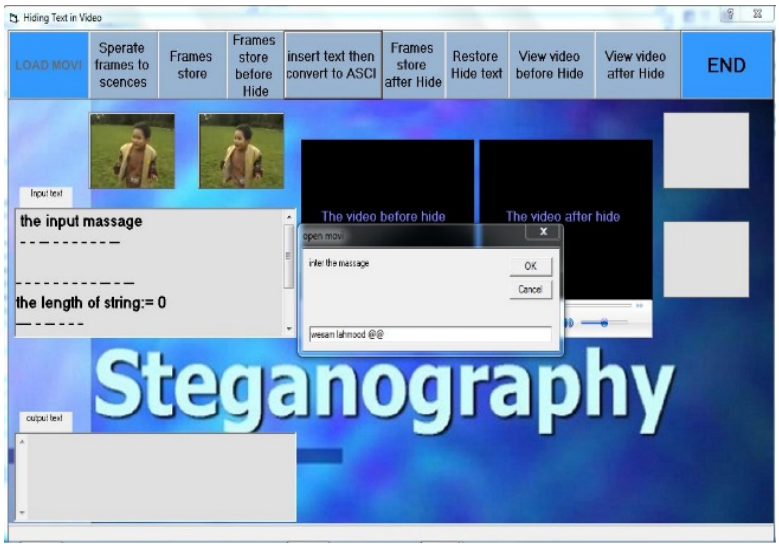


Fig. 9: A form of English and Arabic texts (letters and symbols) was hidden in a video file

Fig. 10: Scenes of video file before the process of hiding: a) Into frame 11; b) Into frame 19; c) Into frame 33; d) Into frame 47 and e) Into frame 53

Fig. 11: Scenes of video file after the process of hiding: a) Into frame 11; b) Into frame 19; c) Into frame 33; d) Into frame 47 and e) Into frame 53

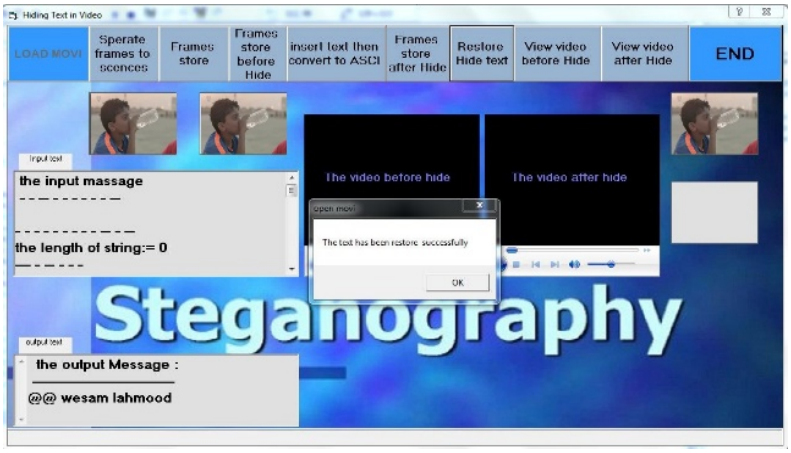


Fig. 12: Recovering the hidden text

Fig. 13: Display the video before and after the hide text

Step 6: In this step, we are recovering the hidden text as shown in Fig. 12.

Step 7: In this step, we display the video before and after the hide text, after we take scenes that we have worked on to hide the text and restored to the video. Figure 13 this process.

CONCLUSION

This research presents a new path in steganography was used file video as a vector text series. Through the design and implementation of the proposed system and discussing its results, we concluded the use of colors that make up the three main colors of the image in the process of concealment provided storage space is greater than the use of a gradient only one. Also, we can take advantage of the large storage space provided by the video file to hide the data with a larger size. The movement show video file will be the biggest obstacle to distinguish any difference which gives greater security for the transfer of hidden data.

RECOMMENDATIONS

In hiding stage it is applicable to use any type of transformations such as Wavelet, DCT and so on, also, we can use other types of video. Finally, we can use of special methods to encrypt data before concealed.

REFERENCES

Gallagher, A.C., 2012. Jigsaw puzzles with pieces of unknown orientation. Proceedings of the 2012 IEEE International Conference on Computer Vision and Pattern Recognition (CVPR), June 16-21, 2012, IEEE, Providence, Rhode Island, USA., ISBN:978-1-4673-1226-4, pp: 382-389.

Haralick, R.M., K. Shanmugam and I.H. Dinstein, 1973. Textural features for image classification. IEEE Trans. Syst. Man Cybern., SMC-3: 610-621.

Karasik, A. and U. Smilansky, 2011. Computerized morphological classification of ceramics. J. Archaeol. Sci., 38: 2644-2657.

Katzenbeisser, S. and F. Petitcolas, 2000. Information hiding techniques for steganography and digital watermarking. Artech House Inc., Norwood, Massachusetts, ISBN:9781580534154, Pages: 239.

Makridis, M. and N. Papamarkos, 2010. A new technique for solving puzzles. IEEE. Trans. Syst. Man Cyb. Cyber., 40: 789-797.

Makridis, M. and P. Daras, 2012. Automatic classification of archaeological pottery sherds. J. Comput. Cult. Heritage, 5: 1-15.

Nados, W.L., R.D. Kumar, D.M.A. Naser and A.A. Hussein, 2014. Medical images classification by using artificial intelligence techniques. Intl. J. Sci. Eng. Technol. Res., 3: 6812-6816.

Oxholm, G. and K. Nishino, 2013. A flexible approach to reassembling thin artifacts of unknown geometry. J. Cult. Heritage, 14: 51-61.

Piccoli, C., P. Aparajeya, G.T. Papadopoulos, J. Bintliff and F.F. Leymarie *et al*., 2015. Towards the automatic classification of pottery sherds: Two complementary approaches. Proceedings of the 41st International Conference on Computer Applications and Quantative Methods in Archaeology, March 25-28, 2013, CAA, Perth, Western Australia, pp: 463-474.

Richter, F., C.X. Ries and R. Lienhart, 2011. A graph algorithmic framework for the assembly of shredded documents. Proceedings of the 2011 IEEE International Conference on Multimedia and Expo (ICME), July 11-15, 2011, IEEE, Barcelona, Spain, ISBN:978-1-61284-348-3, pp: 1-6.

Rousopoulos, P., C. Papaodysseus, D. Arabatzis, M. Exarhos and M. Panagopoulos, 2011. Reconstruction of c.1650 B.C. fragmented wall paintings by exploitation of the thematic content. Intl. J. Imag. Rob., 5: 1-17.

Shin, H., C. Doumas, T. Funkhouser, S. Rusinkiewicz and K. Steiglitz *et al*., 2012. Analyzing and simulating fracture patterns of Theran wall paintings. J. Comput. Cult. Heritage, 5: 1-10.

Stanco, F., D. Tanasi and G. Gallo, 2011. Virtual restoration of fragmented glass plate photographs of archaeological repertoires. Virtual Archaeol. Virtual restoration Rev., 2: 141-144.