

Text Encryption Based on Pixel Value Difference of Video Frame

Huda Ghazie Abd UL Sahib Assist.Prof.Dr. Maisa'a Abid Ali Khodher
University of Technology - Department of computer Sciences –Iraq

cs.19.03@grad.uotechnology.edu.iq
110044@uotechnology.edu.iq

Abstract

The growth of IT and telecommunications is becoming very relevant in terms of safety, security can be performed using steganography, and in the field of information security steganography plays an important role. In this paper, a steganography algorithm is proposed to hiding a confidential message inside a video for the purpose of sending it to another party without attract the attention of attacker and unauthorized parties and with high security and a high embedding rate. This is done by embedding the secret message and distributing it between the video frames in a certain way using steganography techniques.

The proposed method is implemented by using several steps. In first step: it divided the video in number of frames, the next step: is encrypt the secret message using AES algorithm, after encryption process the message is hiding in frames of video, for each ten frames select one frame video to hide secret message in it. And the final steps: is using secret key $(n+5)$ this key is use to determine the locations of the pixels in order to hide bits of secret message in a blue color channel by using pixel value difference (PVD), it uses zigzag columns for hide the encryption secret message in each location based on secret key. In addition to that, the proposed method has removed the limitations of the (PVD) method.

The outcomes of the proposed system are good in security, transparency, efficient, high capacity, and powerful. Because, it uses measurements of peak signal to noise ratio (PSNR), mean square error (MSE), entropy, and correlation coefficient. This system is preventing by attackers to detect the encryption secret message.

KEYWORDS: Steganography, Pixel Value Difference (PVD), Encryption, Secret message, Secret key.

1-Introduction

At the recent years, Internet is becoming a very important common medium for communication. However, confidential data security during transfer through it has become a great challenge. Encryption is the most effective means to achieve security. The secret message can easily have detected by the attacker if the security is not strong enough so, Capacity, reliability and invisibility are critical criteria for confidential data security [1]. There are two schemes to accomplish these goals.

The first is encryption, in which confidential data encoded by means of a secret key, which only similar secret key will decipher. DES, AES, RSA and so on are the most common encryption techniques [2]. However, this scheme will attract people not responsible for the information, the other method used to reduce suspicion is steganography, and Steganography is a method of concealing sensitive information in coverage media [3].

When the cover media is an image or frame, the cover photo or the cover frame that contain the secret data is called stego image. In various applications steganographic technique can be used such as military, commercial, anti-criminal and so on [2].

Steganography is based on the hide of confidential data. The concealment of the secret data into another media in order to protect it against unauthorized access. To increase the security of the data, it can be encrypted before using steganography. Many steganographic methods have been improved over years for different types of cover media: text, image, audio and video [4], [5].

Steganography aims to hide or conceal the existence of secret messages or sensitive information, and concealment, can be accomplished by making reasonable changes to other digital media contents [6]. These modifications are based on the key and the data need to be concealed. The recipient can then extract data confidential by using the same secret key from the algorithm [3], [7], [8].

2-Related work

Many steganographic techniques have been proposed for embedding information in the cover media. Some approaches based on a principle of replacing the pixels' least important bits in the original image and others using an LSB and wavelet technique by increasing or decreasing the transformative image coefficients by one unit [9],[10],[11].

Most of the related researches focus on increasing the capacity by using LSB and the readjustment process, and there are many other study that take different technique like:

In (2016), Rana Tayseer sabbah, proposed uses (PVD) in a gray scale image the pixel value must be in ranges from 0 to 255. But when use this method as image steganographic scheme sometimes the pixel values in the stego-image may exceed gray scale range. The PVD approach divides the original image into two consecutive pixel of non-overlapping blocks and modifies the pixel differential for data embedding in each block (pair). The outcomes of this proposed the PVD is better image quality and capacity of hiding data, and give the complexity and powerful [8].

In (2017), Doli Hasibuan and Junika Napitupulu, proposed Steganography process to insert secret data into images using the pixel-value differentiation algorithm used to insert RGB pixels into an image domain. This algorithm performs the process of inserting the text length of the message, as the images are inserted on the pixel of an image, Concluded that there is no suspicion of the Pixel Value Differencing algorithms, since the message is concealed on an RGB pixel image, and the message length can be hidden as much as the RGB pixels of the image used as media [3].

In (2019), Dipika Deshmukh and Gajanan Kurundkar, proposed uses edge detection techniques in video steganography. The work follows random frame selection algorithms to protect the confidentiality of confidential information. In order to insert data in video frames, the LSB method is used. They have improved data hiding techniques. Concealing in LSB bits alters the pixels' resolution that are convenient for the human eye to observe during detection mechanisms and therefore convenient for attackers. However, their methodology can integrate large numbers of data than LSB. Edge detection is used, edge detection is carried out by various edge detectors [12].

In (2020), Manohar N and Peetla Vijay Kumar, proposed uses secure steganography method, The LSB system, neural networks, and fuzzy logic provide a solid base, Then, using PSNR and MSE, verify their processes. Taking a video stream file is the first step in their process and an SLSB method can be used to create an embed process that becomes a stego file. The fuzzy logic is then applied and the input and output variables are processed in the second step. The implementation of neural networks and the provision of data inputs and outputs are included in the third step. More formats, security, performance quality, and PSNR & MSE accuracy values were finally seen as a result [13].

3-Steganography

Data hiding is the process of embedding confidential data into digital media without causing attracting attention. Three popular techniques can be used in data hiding. They are watermarking, cryptography and steganography [14], [15].

In the hiding information methods, cryptography and steganography are distinct. Cryptography is the science of conversion of secret messages to some other type, so that none other than the intended sender and recipients can understand it.

In the steganographic systems the main terminology is: cover media, confidential message, secret key, and embedding algorithm. The original media is the carrier of messages in pictures, video, audio, text or other digital media. The confidential message is the data that must be concealed in the digital platforms. The embedded algorithms are used to insert the message using the secret key. This algorithm is a method or a concept used to include the secret knowledge in the cover media [16].

In steganography, the sender needs to pick a suitable message carrier, an appropriate message to hide and a secret key to use as a password before hiding. The transmitter will then give the hidden message to the recipient using some of the current communication techniques. The receiver decrypts the hidden message using the extraction algorithm and a secret key after receiving the message [17], the steganography structure is shown in the Fig.1 [18], [19]:

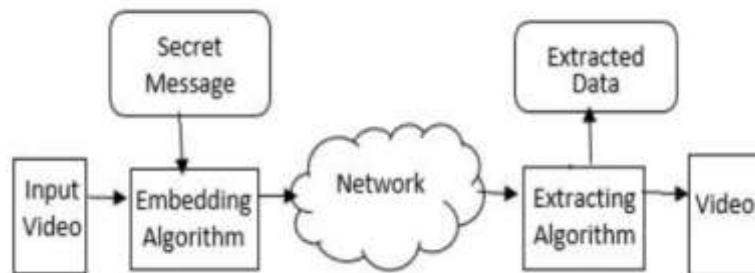


Fig. 1: The structure of steganography technique.

4- Video steganography

Steganography in video is a way of concealing data or messages into frames in video format. Video is a picture or frame combination used to hide text messages. And it is a spatial domain technique, different methods are used to conceal the data from human eyes in various video frames [18]. Different methods on spatial domain used to embed data directly in the cover frame without adjustments and with a good quality such as LSB substitution, Spread Spectrum, Histogram Manipulation, Most Significant Bit (MSB), Quantization Index Modulation (QIM) and pixel value differencing (PVD). Data hidden in video frames now play a major role in steganography for a few days. Steganography's key work is to conceal the hidden message without affecting the visual quality, structure and content of the video file [19], [20].

Video steganography has a much greater potential for hiding sensitive information because video has a large number of redundant bits [21], [22].

Digital video has a range of images played according to video specifications at fixed frame rates. The quality of digital video is determined by a number of factors including fps (frames per second), frame size, and pixel size. The default fps factor is a very common video format. It values respectively 24 and 30 fps. Every video image is called a Frame containing three or four colors in

pixels, such as RGB (Red, Green, Blue) and CMYK (Cyan, Magenta, Yellow and Black). A combination of these primary colors is the remaining colors of the mediator [19]. A pixel consists of three color combination (Red, Green, Blue). A pixel component color contribution is different (Red, Green or Blue). Green contributes 59 percent while the red part supports 30 percent and the blue part contributes 11 percent in a colored point [

5-Pixel Value Difference Algorithm (PVD)

Pixel value difference algorithm proposed by Wu and Tsai to conceal more data with high quality of stego-image or frame and provide more security in data hiding [2], In the PVD algorithm, a gray-value cover frame is partitioned into non-overlapping blocks consisting of two consecutive pixels (p_i, p_{i+1}) [1], The method of splitting the original frame into two-pixel blocks done as a zigzag through all the rows of each frame, As illustrated in Fig. 2[5].

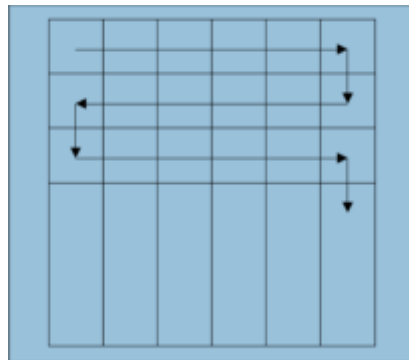


Fig. 2: The two-pixel blocks that do not overlap are created by zigzag scanning the rows by collecting every two consecutive pixels in a cover image

A difference value $|d_i|$ can be determined from each block by subtracting p_i from p_{i+1} . All the differences must be between -255 and 255 . The absolute difference is, however, between 0 and 255 . Per width of the range is taken as a power of 2. There are two types of range the first type is to select a wide range $[8, 8, 16, 32, 64, 128]$ for a high capacity. And the other is a large range of $[2, 2, 4, 4, 4, 4, 8, 16, 16, 32, 32, 64, 64]$ to maintain a high level of imperceptibility [1],[3].

In a proposed method will use $R = \{[0.7], [8.15], [16.31] [32.63], [64.127], [128.255]\}$ Scheme for Tsai and Wu [3]. This method is used to see if the differences are within two pixels of each other, then the number of the bit is to be inserted into a block of two pixels that do not overlap, the amount of bits inserted by the message is done by:

$$\text{Number of bit} = \text{Log}_2(\text{upper width}-\text{lower width}+1)$$

OR by n = number of bit

If	0 <= d_i < 16	then n=3
Else If	16 <= d_i < 32	then n=4
Else If	32 <= d_i < 64	then n=5
Else If	64 <= d_i < 128	then n=6
Else If	128 <= d_i < 255	then n=7

Now computing the new value of pixels this is the embedding process. On the side of the receiver also calculate the difference between the two pixel block from the stego image $d_i' = |p_i' - p_{i+1}'|$. Then the difference d_i' is used to check for the amount of concealed block bit streams using the table of range The hidden bit streams are extracted after the decimal value has been converted to binary

form : secret bit = $(d_i' - \text{lower } i)$ OR by secret bit = $(d_i' - 2^n)$ but if $0 \leq d_i' < 8$ the secret bit = d_i' [٢٣].

The PVD have some limitation this limitation is fall boundary issues [٢٤] that's mean the color pixel value may overtake the range (0-255) in a stego image [٢], in a proposed method removed this issue of PVD method.

6-Proposed method

In this paper, the proposed system aim hiding confidential data inside a video using PVD technique for the purpose of sending it to the other party with high security and a high embedding rate. And there are two main algorithms, which are the embedding algorithm and the extraction algorithm, and in each algorithm there is a set of steps that will be explained in the following sections. Fig. 3 and Fig. 4 to explain detail of each algorithm.

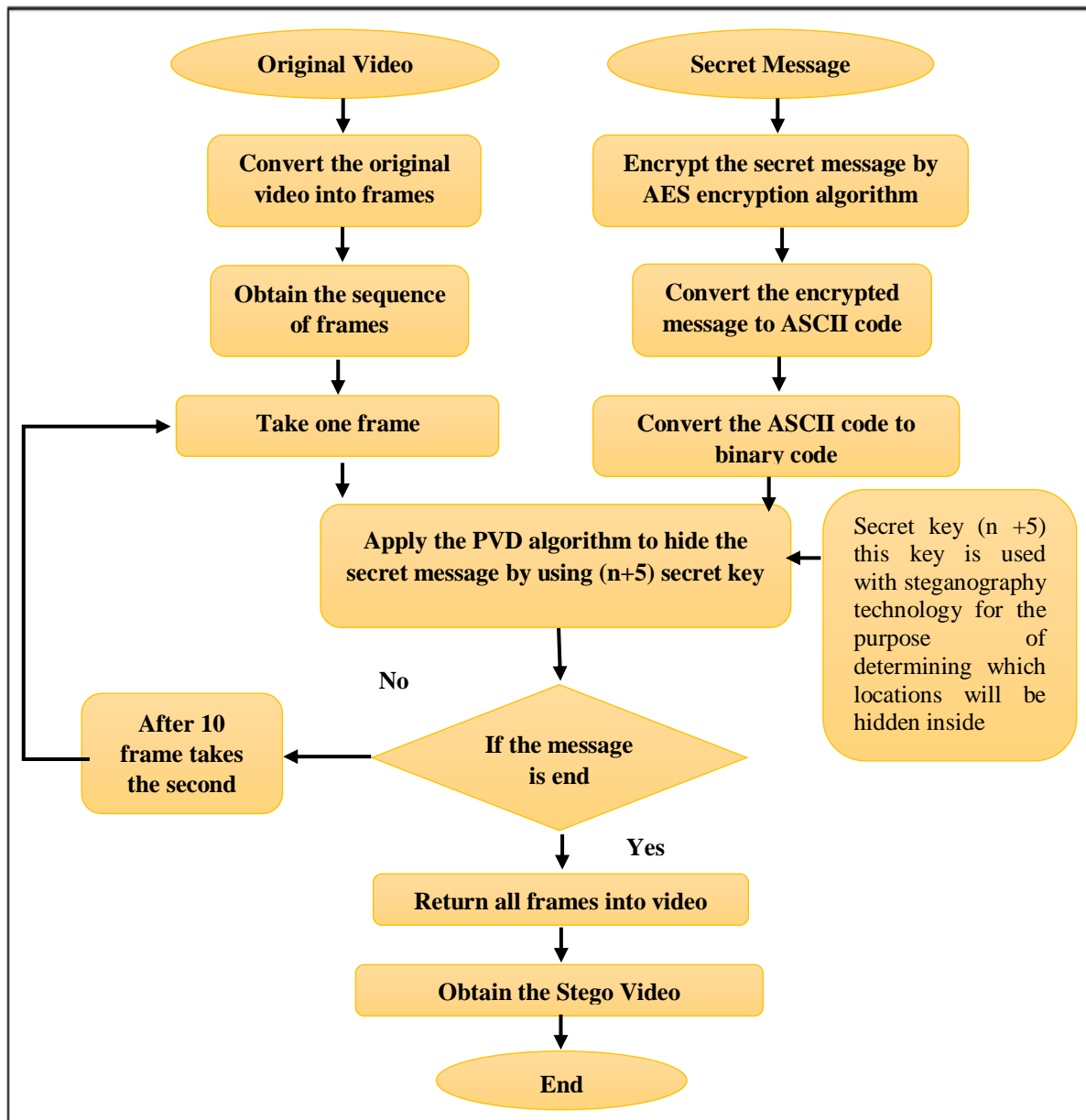


Fig. 3: The embedding algorithm.

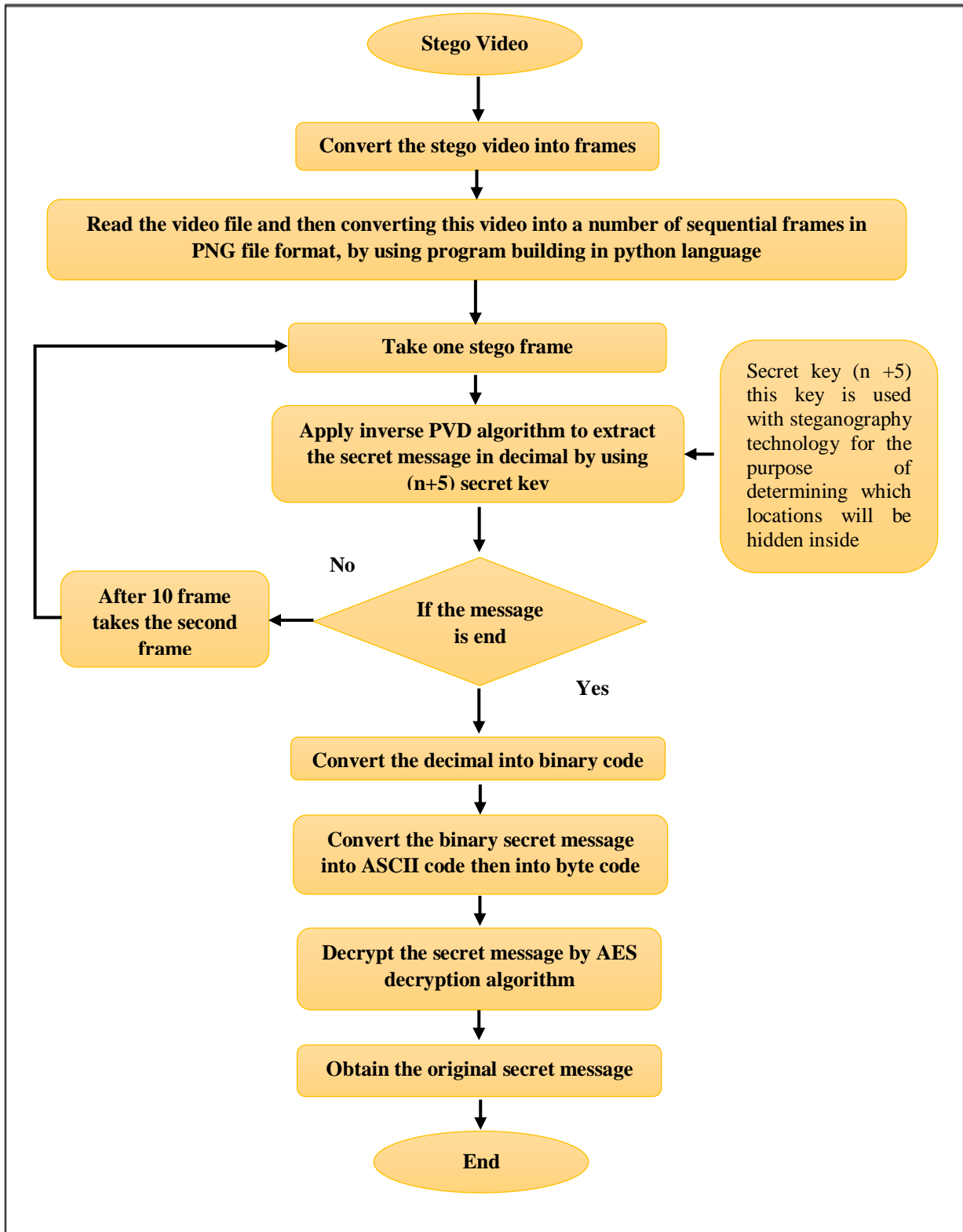


Fig. 4: The extracting algorithm.

6.1 The first step: Divide video

Convert the original video in to a number of frames in this step the video file will be read and then converting this video into a number of sequential frames in PNG file format, it takes one frame from the sequence of frames, and applied the pixel value difference (PVD). As shown in fig. 5.

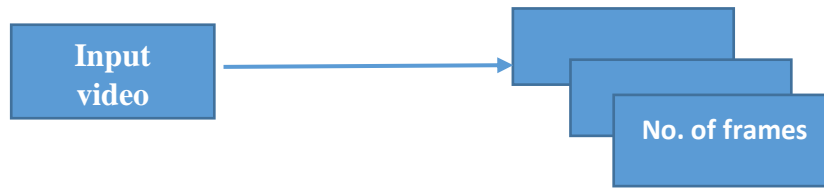


Fig.5: The divide video in no. of frames

6.2 The next step: Encrypted secret message

Encrypted secret message: the secret message will be encrypting by using the (AES) encryption algorithm, this algorithm is implemented by splitting the secret message into 16-byte blocks (128 bit) with using a padding scheme to allow encryption of plaintexts of arbitrary lengths. Each block will enter into four stages, which are bytes of substitution, shift rows, mix columns and add round key, in addition generate a random key with the same size blocks. A byte-coded message will be generated by this algorithm. And after the encryption process is finished, we convert a byte-coded message into list of ASCII code then converting this list into list of binary code. As shown in fig. 6.

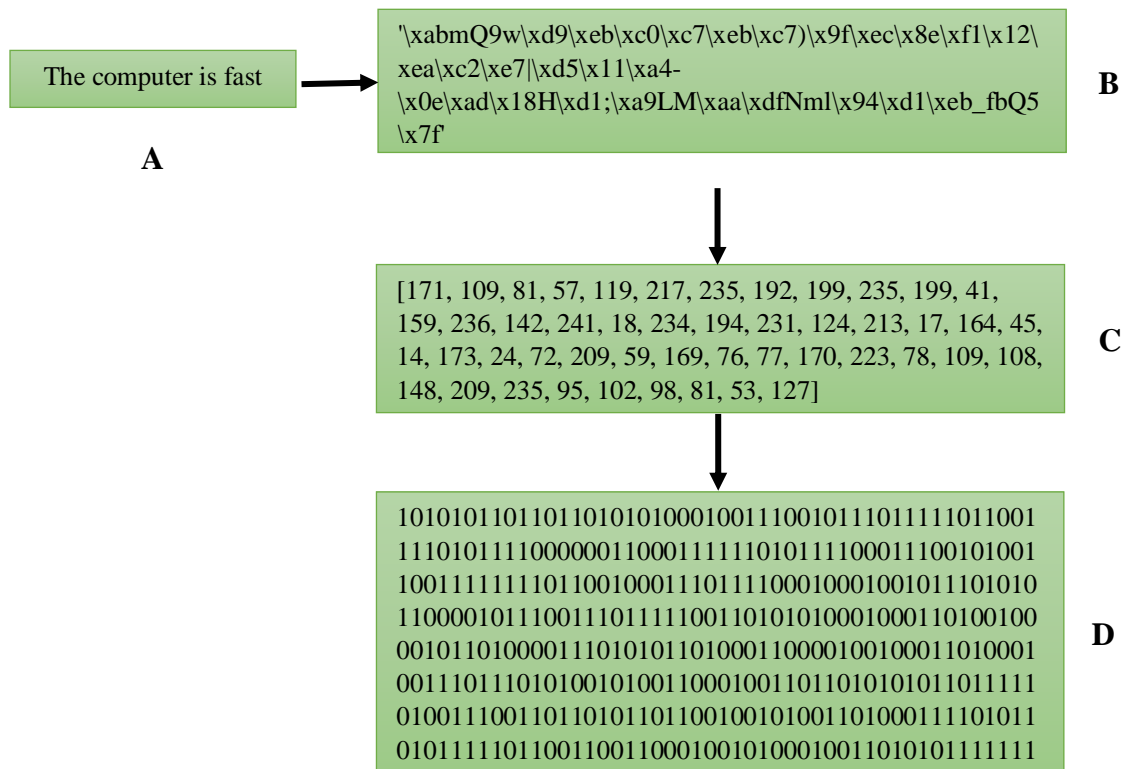


Fig.6: Explain encrypted message in AES, A) original secret message, B) byte code in AES, C) ASCII code of encryption secret message, D) Binary encrypted secret message

6.3 The final step: hiding encrypted secret message

In this step hide encrypted secret message in video frames for applied PVD on each frames. Take each frame that is named here cover frame and apply the algorithm of (PVD) on it, and start with (PVD) algorithm by partition the cover frame into the number of blocks that do not overlap, each

block contain two pixel but these blocks are divided on the basis of the secret key (n+5) this key is use with the steganography technique. It is selected the locations from frames to hide no. of bits in the frame, and the partition will not be done by the traditional method Via all The lines, for each picture or frame and moving as a zigzag, but the partition will be done by zigzag scanning the columns by collecting each two successive pixels in an original picture. As shown in fig. 7. And obtained stego-video. This vertical zigzag with the secret key (n+5) has added strength to the (PVD) algorithm because it will change the traditional method of hiding by using (PVD), which is concealed serially in all rows of the frame. Therefore, the proposed method will make it difficult for attackers trying to discover the locations of the pixels that was hidden inside.

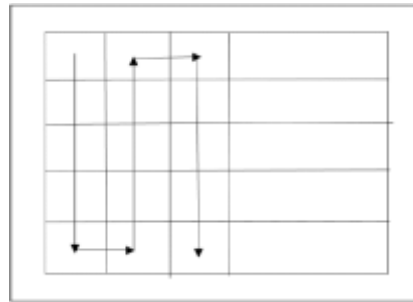


Fig.7: The two-pixel blocks that do not overlap are created by zigzag scanning the columns by accumulating every two pixels in a cover picture

A- Embedding Algorithm:

Algorithm (1): Embedding Algorithm

Input: The original video, secret message

Output: Stego-video

Process:

Step 1: Convert the original video into a number of sequential frames.

Step 2: Encrypted secret message by using the (AES) encryption algorithm. A byte-coded message will be generated by this algorithm. Then convert a byte-coded message into list of ASCII code then converting this list into list of binary code.

Step 3: For I to N // Select one frame from a sequence of frames this is done by taking one frame after every ten shots from the video frames, and the process of taking the number of frames continues according to the length of the secret message. If the secret message is short, it can be hidden with one frame, but if the message is long, it can take more frames, and therefore determining the number of frames is dynamic according to the length of the message.

Step 4: Divide the frame into blocks and on the basis of a vertical zigzag and using secret key (n+5) and thus this key will determine which locations will be used to hide message in the frame.

Step 5: Choose the blue color in order to hide in it // because the human eye is sensitive to the green color, so we decided to use the blue color for hiding in order not to notice any distortion or change in the stego frame.

Step 6: For each pair of pixels

Step 7: $\text{abs}(p_{i+1} - p_i)$ // Calculate the difference between the pair of pixels (p_i, p_{i+1}), then take the absolute value of the different after that determine how many bits will be withdrawn from the secret message, using the range table =([0, 7],[8, 15], [16, 31],[32, 63],[64, 127], [128, 255]).

Step 8: Calculate the new difference value for the pair of pixels and new pixels value

Step 9: Modifying the limitation in the (PVD) algorithm // eliminates the limitation that was in the original algorithm because after computing the new values, may exceed the specified values of the pixels, which are the range (0-255) in stego frame

Step 10: End for (each pair of pixels)

Step 9: if (message is end) **then**
 Go to step 11.
 Else
 $I = I + 10$

Step 10: End for

Step 11: Collected all frames to recreate the stego-video

End.

B- Extracted Algorithm:

Algorithm (2): Extracting Algorithm

Input: The stego video

Output: Original secret message

Process:

Step 1: Convert the stego video into a number of sequential stego frames.

Step 2: Select one Stego frame after every ten shots from the video frames

Step 3: Apply inverse PVD by calculate the difference value $d_i = |p_i - (p_{i+1})|$ and obtain the secret bits decimal = $d_i - \text{lower}_i$ in order to extract the encrypted secret message in a binary code.

Step 4: Apply inverse AES algorithm after convert the binary code into ASCII code then into byte code.



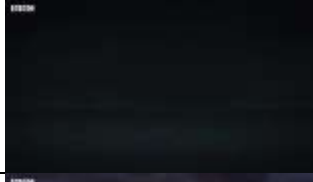
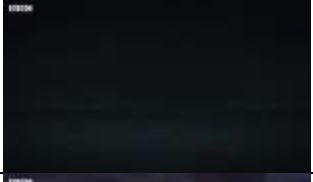






Step 5: Obtain the original secret message

End.

7-Test of the result

This section talks from implementation of each frame in video after hide encryption image, as shown in Table 1. And using a set of measurement PSNR, MSE, Entropy, and correlation coefficient. These are measurement explain in Table 2.

Table 1: indicates for implementation of stego-frame video.

Name of video frame	Original video frame	Stego- video frame
0		
10		
20		
30		
40		

It's noticed in the table 1, which shows the original frames before the embedding process and the stego frame after the embedding process, we note that the image quality has not changed and no distortion can be observed in the stego frame, and this proves the strength of the method by achieving high quality, accuracy and transparency.

Table 2: Indicates for measurements of PSNR, MSE, Entropy, Correlation coefficient.

Name of video frame	PSNR for each frame	The ratio of (PSNR) to the frames	MSE	The ratio of (MSE) to the frames	Entropy	Correlation coefficient
Original video frame(0)	17.5981	84.0655 dB	50.1631	0.00026	6.1187	0.9974
Stego- video frame(0)	17.5954		50.1631		6.1187	0.9995
Original video frame(10)	17.5488	83.9082 dB	10.0872	0.00025	4.2907	0.9884
Stego- video frame(10)	17.5560		10.0872		4.2908	0.9680
Original video frame(20)	17.8239	83.8609 dB	67.7361	0.00026	7.2662	0.9965
Stego- video frame(20)	17.8195		67.7361		7.2662	0.9980
Original video frame(30)	17.9009	83.9741 dB	69.7908	0.00026	7.3252	0.9978
Stego- video frame(30)	17.9062		69.7908		7.3252	0.9983
Original video frame(40)	17.9588	84.2287 dB	71.0789	0.00024	7.4326	0.9991
Stego- video frame(40)	17.9551		71.0789		7.4325	0.9977

It's noticed in the table 2, a very good results in (PSNR) when we compare between the original and stego frame, as it ranges from (83.8609 dB) to (84.2287 dB) and obtain a low (MSE) and notice a little increment in correlation coefficient and good result of Entropy .

8-Comparison with Previous Works

In this section, some comparisons with previous works are done to show the differences in techniques, tools, color channel and security. Table 3 presented the results of comparisons.

Table 3: Indicates comparison results.

References	Tools	Steganography technique	Color channel	security	PSNR	MSE
proposed method	Use video for the purpose of concealment	PVD	Select Blue channel from RGB	AES	84.2287 dB	0.00024
Ref.[8]	Using 256 Gray-valued image	PVD	Gray	Non	38.5359 dB	9.1094
Ref.[15]	Using image	Using a novel steganography algorithm	RGB channel	username and Password are required prior to use the system.	81.47 dB	Non
Ref.[22]	Use video for the purpose of concealment	Hash LSB	RGB channel	Non	60.21 dB	0.061

It's noticed that, PSNR of the proposed algorithm is close to 84dB, which mean very acceptable results, and the proposed method used AES algorithm to encrypt the secret message this means that it achieves high security to maintain the confidentiality of data sent to the other party. In addition obtain low MSE which is refers to high transparency.

9-Conclusion

The pixel value (PVD) approach was used for this article ,with the key represented by (n+5) to hide an encrypted text in a video after divided this video to many frames in order to increase security while transfer the encrypted text and increasing the capacity because this video carried big data.

Many measurements are used in purpose to know the error ratio and the quality of the image and this measurement is PSNR, MSE, Correlation coefficient and Entropy.

As a conclusion there is not error ratio in the frame and there is a good quality while comparison between the stego frame and the original one. These results were examined on a 30-second video with 25 fps and this video is in (mp4) format, this video contain 256 frames each frame size is (1280*720 pixels), in addition the proposed method decided to embed secret message into blue channels of each frame, which reduces the distortion of the pixels in stego frame because each frame is a color image, as each pixel consists of three color combination (Red, Green, Blue). A pixel component color contribution is different (Red, Green or Blue). Green contributes 59 percent while the red part supports 30 percent and the blue part contributes 11 percent in a colored point. Finally this method is a very good to hiding the confidential data with a high capacity, quality, efficiency, transparency, robustness, powerful and security in a video the attacker or unauthorized person cannot detected any suspicious differences in a stego video.

References

- [1] M. A. hameed, Hassaballah, S. Aly, A. S. A. Rady,"A High Payload Steganography Method based on Pixel Value Differencing", Informatics and Systems (INFOS 2018), <https://doi.org/10.1145/nnnnnnn.nnnnnnn>.
- [2] J. k. Mandal, "Colour Image Steganography based on Pixel Value Differencing in Spatial Domain," International Journal of Information Sciences and Techniques, vol. 2, no. 4. pp. 83–93, 2012, doi: 10.5121/ijist.2012.2408.
- [3] D. Hasibuan, J. Napitupulu," Pixel Value Differencing Algorithm in Steganography Image", International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 03, Issue 04; April - 2017 [ISSN: 2455-1457], pp: 98-101

- [4] E. M. El-Alfy, A. A. Al-Sadi, "Pixel-Value Differencing Steganography: Attacks and Improvements", ICCIT 2012, pp: 757-762.
- [5] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10. pp. 1613-1626, 2003, doi: 10.1016/S0167-8655(02)00402-6.
- [6] K. Jung, "Data Hiding Scheme Based on Pixel-Value Differencing in Dual Images", Basic Science Research Program through the National Research Foundation of Korea (NRF) (No. 2015R1D1A1A01058019), 2015.
- [7] Ki-Jong Kim, Ki-Hyun Jung¹, Kee-Young Yoo," A High Capacity Data Hiding Method using PVD and LSB" ,2015 , DOI: 10.1109/CSSE.2008.1378 • Source: IEEE Xplore
- [8] R. T. Sabbah,"A Comparable study of hiding information in images using least significant bit (LSB) substitution and pixel value difference (PVD) Methode",2016.
- [9] J. Kaur and J. Kaur, "Hiding Text in Video Using Steganographic Technique - A Review," vol. 17, no. January. pp. 578-582, 2016.
- [10] M. M., A. A., and F. A., "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection," International Journal of Advanced Computer Science and Applications, vol. 7, no. 3. 2016, doi: 10.14569/ijacsa.2016.070350.
- [11] P. Srilakshmi, C. Himabindu, N. Chaitanya, S. V. Muralidhar, M. V. Sumanth, and K. Vinay, "Text embedding using image steganography in spatial domain," International Journal of Engineering and Technology(UAE), vol. 7, no. 3. pp. 1-4, 2018, doi: 10.14419/ijet.v7i3.6.14922.
- [12] D. Deshmukh,G. Kurundkar , " Video Steganography using Edge Detection Techniques", International Conference on Communication and information Processing (ICCIP-2019), pp:1-4 , <https://ssrn.com/abstract=3419252>
- [13] N. Manohar and P. V. Kumar, "Data Encryption Decryption Using Steganography," Proceedings of the International Conference on Intelligent Computing and Control Systems, ICICCS 2020. pp. 697-702, 2020, doi: 10.1109/ICICCS48265.2020.9120935.
- [14] M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. S. Reddy, , M. Venkatesh," Digital Video Steganography Using LSB Technique", APR 2020 | IRE Journals | Volume 3 Issue 10 |, pp:14-17.
- [15] R. Ibrahim and T. S. Kuan, "Steganography Algorithm to Hide Secret Message inside an Image," Computer Technology and Application, vol. 2. pp. 102-108, 2011.
- [16] A. K. H. Al-Saedi, "A method to hide text in image," Journal of Missan Researches, vol. 12, no. 24. pp. 11-23, 2016.
- [17] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4. 2013.
- [18] A. John, A. Baby,"A Survey on Video Steganography", International Journal of Science and Research (IJSR) ISSN: 2319-7064, Volume 8 Issue 4, April 2019, pp: 800-805 <http://www.ijsr.net>
- [19] K. U. Singh," Video Steganography: Text Hiding in Video by LSB Substitution", Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 4, Issue 5(Version 1), May 2014, pp: 105-108, <http://www.ijera.com>
- [20] G. Nikam, Ankit Gupta, V. Kalal, P. Waghmare," A Survey of Video Steganography Techniques", Journal of Network Communications and Emerging Technologies (JNCET), Volume 7, Issue 5, May (2017), pp: 33-35, <http://www.jncet.org>
- [21] P. V. Shinde, T. B. Rehman," A Survey : Video steganography techniques", International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015 ISSN 2091-2730, pp:1457-1464,[http:// www.ijergs.org](http://www.ijergs.org)
- [22] Deshmukh,B. Rahangdale," Data Hiding using Video Steganography", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April - 2014, pp:856-860. [http:// www.ijert.org](http://www.ijert.org)
- [23] S. Prasad , A. K. Pal," An RGB colour image steganography scheme using verlapping block-based pixel-value differencing", royal society open science, 2017, pp:1-14 [http:// rsos.royalsocietypublishing.org](http://rsos.royalsocietypublishing.org).
- [٢٤] A. K. Sahu, G. Swain," Digital Image Steganography using PVD and Modulo Operation", INTERNETWORKING INDONESIA JOURNAL, ISSN: 1942-9703 / CC BY-NC-ND, (2018), pp: 3-13.