

Comparison of Three Proposal Methods in Steganography Encryption Secret Message using PVD and MapReduce

Huda Ghazie Abd UL Sahib¹, Maisa'a Abid Ali Khodher²

¹²Department of computer sciences, University of Technology, Baghdad, Iraq

¹cs.19.03@grad.uotechnology.edu.iq, ²110044@uotechnology.edu.iq

Abstract: This paper will present a comparison between three proposed methods. All of these methods include hiding a secret message inside a video for the aim of transferring it to another party with high security and a high embedding rate in order to ensure that the secret message is not discovered by the attacker. In addition, facilitating deals with video frames as large data for the purpose of analyzing, dividing and controlling frames easily by the programmer, using the MapReduce method. This is done by dividing the video into a series of frames, and before the hiding process, the message is encrypted using the advance encryption standard (AES) algorithm. These basic processes are implemented in all three proposed methods, the rest of the details for each method are:

The first method: used the pixel value difference (PVD) algorithm to hide the secret message in the video. In addition, the stego secret key was also used. This key is used for the purpose of deciding the locations of the pixels that will be employed to hide the secret message inside it.

The second method: the MapReduce principle is used for the purpose of facilitating dealing with video frames. The chosen frame will enter the MapReduce stages. This is implemented by dividing the frame into three matrices red, green, blue (RGB). Each matrix represents a map. Moreover, the technique that is used for concealment is the least significant bit (LSB) technology which uses the stego secret key (x2) for the purpose of selecting sites that will be hidden by it.

The third method: Also, the MapReduce principle is used, but this method is implemented by dividing the frame into four blocks. Each block represents a map. In one of the stages of the MapReduce, the hiding process will be done by using the (PVD) method which uses the stego secret key (n+15). Finally, the reducer, which is the last stage, will collect the results of each block to generate the stego-frame.

The results of the three methods are efficiency, transparency, robustness and powerful in stego video. It is noticed that the second method has achieved the lowest capacity, thus achieving high security. As for the third method, it achieved the highest capacity and the highest execution time was the first method. Despite this, all the three methods have achieved high security. The attacker or unauthorized person cannot detect any suspicious differences in a stego video. These results are obtained through using many measurements: peak signal-to-noise ratio (PSNR), Mean Squared Error (MSE), Entropy and correlation coefficient.

Index Terms—steganography, PVD, LSB, MapReduce, Secret key.

I. INTRODUCTION

In the digital information interval, big data have emerged as a research area to accurately handle the vast amounts of data produced. Scientifically, these data are exceedingly complex for storage, processing and study using conventional bases of data [1],[2]. Parallel computing paradigms, such as the MapReduce method, have been demonstrated to be a viable solution to this issue [3],[4].

MapReduce is a very powerful, fault tolerant, scalable and simple framework for managing huge quantities of data which can make processing in a simple fashion [5].

After dealing with the big important data and processing them in a parallel to increase the speed of execution, so the next phase must be ensuring how to protect these data during the transmitted over internet and communication, Therefore the security of that information from harmful powers and unauthorized users is also necessary [6]. In general, it is necessary to keep secret messages secure during the transmission. There are two different ways to satisfying that. One way is encryption that applied to encoding procedure of confidential data, in that only the right person with the right key can successfully decode and retrieve the original data [7],[8]. Another way is data hiding, In other words, it is the method of injecting information without causing perceptual degradation into media files. Two popular techniques in data hiding can be used which are steganography and watermarking [9].

Steganography is known as the art and science of writing secret messages in such a way that only the intended recipient is aware of their existence [10]. Steganography must satisfy the basic requirement of capacity (that refers to the amount of data bits concealed in the cover media), the quality of stego images, which must be unchanged, security and robustness. This is what resistance to improvement or destruction [11],[12].

Steganographic approaches may be classified as a spatial domain or a frequency domain. Frequency domain means transforming images into frequency components. In the spatial domain, depending on the intensity of the pixels, information is concealed directly [12]. A widely used spatial domain method is the least significant bit (LSB) and pixel value difference (PVD). PVD was proposed as a way to hide more data while maintaining the high quality of stego image pixels, and this is done by partitioning the original image into non-overlapping blocks of two consecutive pixels [8],[9],[12].

In the systems of steganography, the basic words used are the cover media, secret message, secret key and embedding algorithm. Cover media includes text, audio, video, image, and other media digital contents. The hidden message is the confidential data that must be concealed in the digital media. In general, the secret key is used to embed the message according to the hidden algorithms. The embedding algorithm is the process or the concept used to insert hidden knowledge into the cover letter [10],[13].

Video steganography was employed in this research. Video steganography is an important aspect of steganography since it is an efficient way for hiding data in video frames. It is also important to safeguard our data or knowledge from intruders, hackers, or unauthorized access [14],[15],[16].

II. RELATED WORK

There are numerous studies and researches on the subject of dealing with big data and how to keep these data safe. This paper will take the MapReduce system that demonstrates how to deal with and process big data and take the researches about the steganography technique that hide and provide a good security to the important data and information.

In (2017), Seyed Nima Khezr and Nima Jafari Navimipour. Their paper proposed a research about analyzes MapReduce application and implementation in various contexts such as cloud, multi-core and concurrent computing precise investigation were carried out. The main point of their article is to describe MapReduce, its design, big amount of data and the efficient use of the programming model by the application. In addition, it examines a variety of applications and classifies them surveyed under the MapReduce System join and parallel requests, focused on graph processing, frameworks, multi-core frameworks and data optimization Allocation [5].

In (2017), Doli Hasibuan and Junika Napitupulu. Their paper proposed a research that explored the steganography method to insert messages in images using a pixel value difference algorithm that has been inserted into RGB pixels in an image. They concluded from their research that the pixel value

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

differencing algorithm is not suspicious as it could conceal the message on the RGB pixel and message length as well as the RGB image pixels used as media pixels [15].

In (2018), P. Srilakshmi and et al. Their paper proposed a method to image steganography for the spatial domain embedding of text. The message is dumped into the image with a randomly generated key in the suggested image, on the basis of which text is extracted from the image. So this approach is extremely guarded and difficult to classify the text information in the image and to extract the secret message from the image is also a rigorous operation. Extraction can only be achieved if the key is known [17].

In (2018), Aditya Kumar Sahu and Gandharba Swain. Their paper proposed an image steganography method by using the concept of pixel value difference (PVD) and modulo operation (MO). The key components of the ideas proposed by the solution are: (1) improving the peak signal-to-noise ratio (PSNR), (2) increase in available hiding capacity, (3) Prevention of fall off boundary issue. The first step involves partitioning the image into non-overlapping blocks which, in turn, are composed of three consecutive pixels. The hidden information is then embedded in a block. For the second step, the average value of the first two stego-pixels of the block and the third pixel is computed for data embedding using PVD method. The performance of the method that has been presented is compared to existing approaches and was found to be better [18].

In (2020), Ibrahim Abaker Targio Hashem. This paper is intended to examine the research that is carried out in the field of planning on big data platforms. This paper examined preparation on two aspects in MapReduce: taxonomy and performance assessment. His analysis can be the benchmark for experts to suggest a novel algorithm for scheduling MapReduce. However the analysis can be used as a starting point for beginner researchers [4].

In (2020), M. Venkata Sai Tarun and et al. Their paper showed encryption of compressed video bit streams and information concealed for video security during transmission. To prevent the video from being manipulated, Bit replacement was used to embed hidden message bits with compressed bit streams [19].

In (2020), Ashwak Alabaichi and et al. Their paper proposed a method for image steganography using least significant bit and secret map techniques is performed by applying 3D chaotic maps, namely, 3D Chebyshev and 3D logistic maps to obtain high security. Results showed that the proposed algorithm satisfies all the aforementioned criteria, it is efficient in hiding secret data and preserving the good visual quality of stego images [12].

III. VIDEO STEGANOGRAPHY

Video steganography is an instrument for concealing data in video frames [19]. Various methods are used to hide the secret data in video frames safe from the human eye [20],[21]. Since video files contain many frames and have more storage space, they can hide more detail than audio and image files [22],[23].

A sequence of frames plays at a fixed frame rate in digital video. The frame rate is defined by the type of video. Digital video quality depends on parameters such as fps, the amount of pixels in a frame and the size of a frame [24],[25]. The standard fps parameter is general video formats, with a value between 24 and 30 fps, but two other parameters are improved from one video format to another, as are the number of pixels in a frame and frame size. Each picture in a video is a frame with three or four colored combinations of pixels such as RGB (Red, Green, Blue) or CMYK (Cyan, Magenta, Yellow, Black). The remaining colors of the mediator consist of a combination of these primary colors [26],[27],[28].

The use of video as a cover medium has the advantage of allowing data to be stored in vast quantities of space. Since the video file is much more complicated than the image file, there is more security

Received 22/4/2021; Accepted 25/6/2021

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

against the intruder. Another advantage is that the secret data are insignificant to human eye because pixel color varies [29],[30].

There are two steps to video steganography. The first step is to insert the hidden message into the video files. The second step is hiding message extraction from video files [31]. After hiding information in a video file in several frames, these frames are combined to create a stego video, which looks like a regular video. The authorized recipient performs the reverse process to extract the secret message or data from the video [23],[32]. The video steganography in this paper using the pixel value difference PVD and LSB insertion technique is developed in PYTHON. The video steganography block diagram is seen in Fig .1.

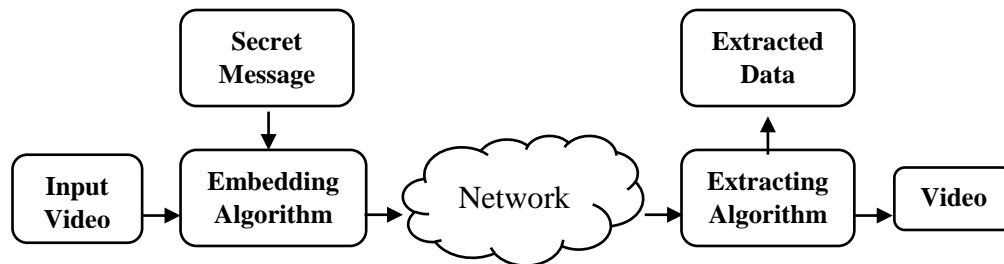


FIG. 1: THE VIDEO STEGANOGRAPHY BLOCK DIAGRAM

IV. PIXEL VALUE DIFFERENCE ALGORITHM (PVD)

Wu and Tsai proposed a steganography process called pixel value difference. The high embedding ability and outstanding imperceptibility of the stego images can be effective in this method [33] [34]. It was considered as a good steganographic algorithm because of its high payload and good visual perception in the spatial domain [35].

Initially, the Pixel Value Differencing (PVD) method was proposed to hide messages in images with 256 gray values. It can add large amounts of data without degrading image quality, so human eyes don't recognize them. PVD specifies the amount of message bits to be inserted in each pair of pixels based on the difference between them [36].

At first the image is partitioning into blocks that do not overlap by two consecutive pixels, p_i and p_{i+1} [8],[37].

The differential value d_i is determined from each block via subtracting p_i from p_{i+1} . The collection of values for all the differences may vary from -255 to 255. Thus, $|d_i|$ ranges from 0 to 255. The small difference value blocks are found in the smooth region where the sharp edged area is the block with high differential values. More data can therefore be embedded into the edge than smooth areas. Therefore a range table was designed in the PVD method. The Wu and Tsai method involves two forms of range tables. The first one of these is to pick a wide range [8, 8, 16, 32, 64, 128] to have a high capacity. The second one is chosen to give high imperceptibility with a broad range of [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64] [8],[15], this range is used to decide the length of bits to be embedded [38]. In two consecutive pixels the number of hidden bit sequences (n) depends upon the table and is determined as [39]:

Number of bit = $\log_2(\text{upper width} - \text{lower width} + 1)$ OR by n = number of bit

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

Received 22/4/2021; Accepted 25/6/2021

The series of bits obtained is transformed to decimal the value then new different value is calculated using the equation: $di' = \text{lower width} + b$ OR by $di' = 2^n + b$ but if $0 \leq di < 8$ then $di' = b$. The adjusted pixel values are determined on the basis of the following condition:

$$\text{New value of } (P_i, P_{i+1}) = \begin{cases} (P_i + \text{ceiling}(\frac{m}{2}), P_{i+1} - \text{floor}(\frac{m}{2})), & \text{if } P_i \geq P_{i+1} \text{ and } d'_i > d_i \\ (P_i - \text{floor}(\frac{m}{2}), P_{i+1} + \text{ceiling}(\frac{m}{2})), & \text{if } P_i < P_{i+1} \text{ and } d'_i > d_i \\ (P_i - \text{ceiling}(\frac{m}{2}), P_{i+1} + \text{floor}(\frac{m}{2})), & \text{if } P_i \geq P_{i+1} \text{ and } d'_i \leq d_i \\ (P_i + \text{ceiling}(\frac{m}{2}), P_{i+1} - \text{floor}(\frac{m}{2})), & \text{if } P_i < P_{i+1} \text{ and } d'_i \leq d_i \end{cases}$$

Where $m = |di' - di|$ 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 $di' = |p_i - p_{i+1}|$. Then the difference di' 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 = $(di' - \text{lower } i)$ OR by secret bit = $(di' - 2^n)$ but if $0 \leq di' < 8$ the secret bit = di' [34]. The embedding process by PVD algorithm is illustrate in fig.2.

The PVD have some limitation, this limitation is fall boundary issues [18]. This means that the color pixel value may overtake the range (0-255) in a stego image [8], in a proposed method removed this issue of PVD method.

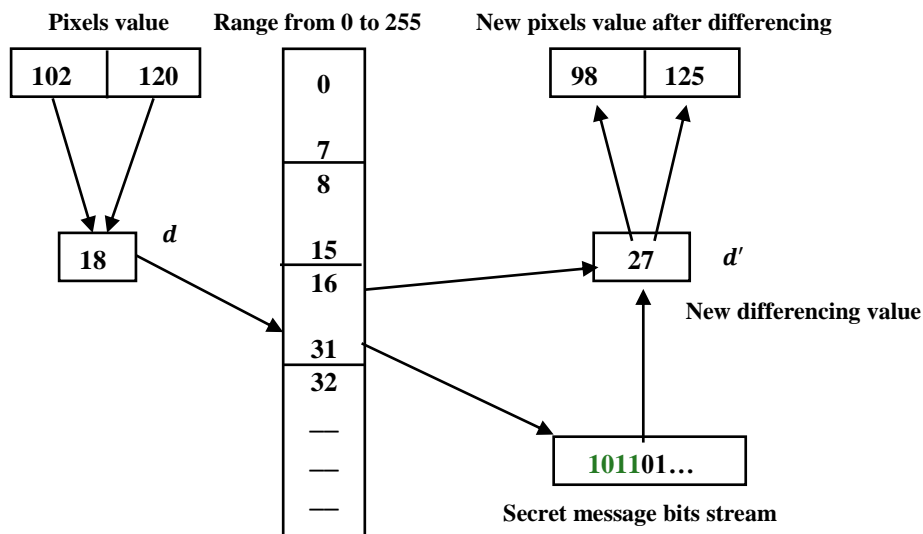


FIG. 2: THE EMBEDDING PROCESS BY PVD ALGORITHM

V. MAPREDUCE

The overabundance of data and information made the analysis difficult [15]. To meet the demands for data analysis, new techniques in software, hardware, and algorithms are needed [16]. A number of parallel algorithms were developed using various parallel approaches that can be described as: MapReduce, threads, MPI and mash-up or workflow technology that offers various usability and efficiency features [2]. MapReduce is a common technique for massive data processing such as distributed and scalable. It is being used increasingly in various applications due to its significant characteristics, including scalability, fault tolerance, ease of programming and flexibility [1].

MapReduce is a programming model for writing application that can process Big Data on multiple nodes in parallel [17]. MapReduce is designed for programmers instead of business users. It's a

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

programming model, not a programming language. It has become popular because of its simplicity, efficiency and ability to monitor big data a timely way.

Applications that involve concept of indexing and searching, graph and text analysis, machine learning, data manipulation and many more are difficult to accomplish using standard DBMS SQLs. In these fields, the procedural nature of MapReduce makes it easy for trained programmers to understand [2].

The basic architecture of MapReduce as the following:

MapReduce is implemented in a node cluster, with one node serving as a master and the other nodes acting as workers. Nodes of workers are responsible for map and reduce tasks running [1]; and the main three components of MapReduce are: Master, Map function and Reduce function. The master is accountable for allocating assignments to workers (mapper, reducer). A MapReduce application has a job workflow in which two user-specified functions are generated, namely Map and Reduce. Each input record is added to the Map function and a list of intermediate records is generated. The Reduce function (also known as Reducer) is used to construct an output list for any intermediate record category with the same key. Therefore, in order to take a close look at each phase:

- Input step (master) - For map and reduce tasks, the master is in charge of preserving and supplying data and procedures. it is a record reader which divided every record in an input file. It can be specified as a key-value pair, then sent data to the mapper.
- Mapper - A Mapper takes input data from the master and transforms them to a pair of key/value pairs.
- Intermediate keys - the mapper produced key value pairs are known as intermediate keys.
- Shuffle and Sort - In MapReduce, the Map task has already been completed, large quantities of intermediate data are normally transferred from all Map nodes to all Reduce nodes in the shuffle process, the shuffle pass data from the Mapper disks and the intermediate result will be sorted by keys so that all pairs with the same key are grouped and the data from the local Map nodes are transferred to reduce nodes.
- Reducer - Reducer takes an intermediate key as well as a collection of key values. This combines these values to form a smaller set of values.
- Output phase - The final key value pairs will be translated from the reducer function and written to an end file during the output process [5]. The basic architecture of MapReduce is seen in the Figure below.

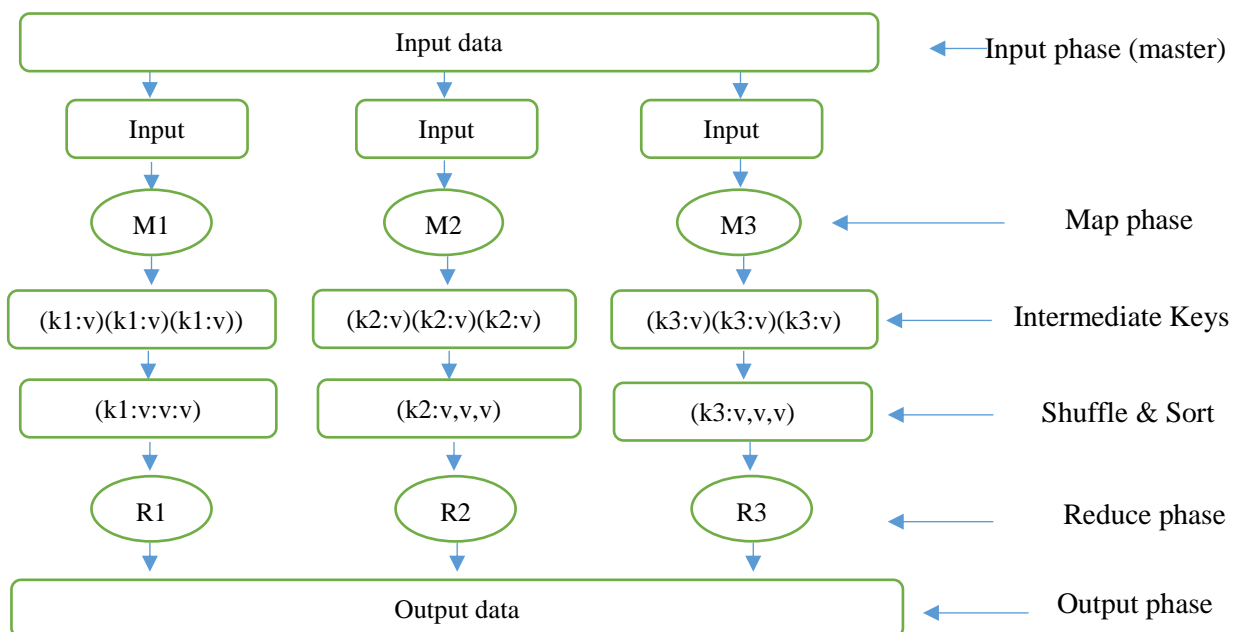


FIG.3: THE BASIC ARCHITECTURE OF MAPREDUCE

Received 22/4/2021; Accepted 25/6/2021

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

MapReduce is used in many applications for massive data [1], it is used in optimization algorithms such as genetic algorithm and Ant colony algorithm and so on [2], and it is also used in other applications such as Uniform Resource Locator (URL frequency count): The map function processes the login to web page and requests of key value pairs of (URL, 1). URL. The reducing function adds all values together for the same URL, and the (URL, total count) is emitted [3].

Another popular example is the word count application. Word count is regarded as a MapReduce program that counts the number of times each word appears in a text document and gets a sample from a huge set of results and analyzes them [5]. In the proposed methods, the MapReduce algorithm will be used for steganography to deal with hiding encrypted secret message in a video by using many steps because the video provides a big size to conceal a large amount of data.

VI. PROPOSED METHODS

In this paper, three methods have been suggested and comparison has been done between them, and the main goal of these three methods is 1- Hiding confidential data inside a video using concealment techniques for the purpose of sending it to the other party with high security and a high embedding rate. 2- Facilitating dealing with video frames as large data for the purpose of analyzing, dividing and controlling frames easily by the programmer, using the MapReduce method.

In any of the three proposed methods, 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.

I. Embedding Algorithm

The embedding algorithm includes several steps which are:

- **The first step (in each three proposed method):** converting the original video into a number of sequential 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, each frame size is (1280*720 pixels). As shown in fig. 4.

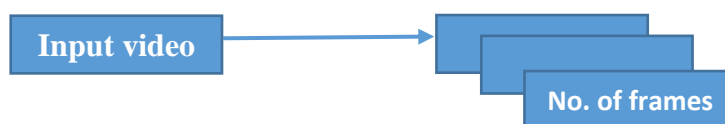


FIG.4: CONVERTING THE ORIGINAL VIDEO INTO A NUMBER OF SEQUENTIAL FRAMES

- **The second step (in each three proposed method):** 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 adding round key, in addition to generating a key with the same size blocks. A byte-coded message will be generated by this algorithm. And after the encryption process is finished, a byte-coded message is converted into list of ASCII code then converting this list into list of binary code. Then this list will be merged into a chain of Binary Bit. As shown in Fig. 5.

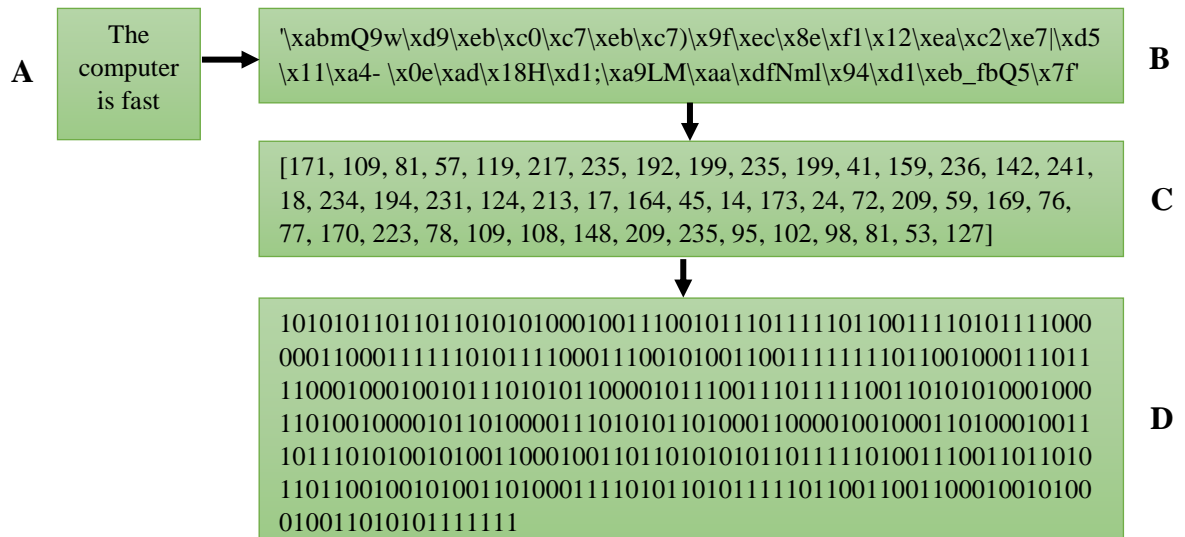


FIG.5: EXPLAIN ENCRYPTED MESSAGE IN AES, A) ORIGINAL SECRET MESSAGE, B) BYTE CODE IN AES, C) ASCII CODE OF ENCRYPTION SECRET MESSAGE, D) BINARY ENCRYPTED SECRET MESSAGE.

- **The third step (in each three proposed method):** select one frame from a sequence of frames: in this step will be choosing the frames that will be used for the purpose of hiding in them from within the video frame series. The frame selection process 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.

- **The fourth step : The fourth step is different according to the method**

1- **The first method:** applying the pixel value difference algorithm on the selected frame. Firstly, this algorithm, divides the frame into non-overlapping blocks, and each block contains a pair of pixels, and these pairs are identified using the secret key $(n+15)$ where blocks will not be taken in sequence, but between each block and other 15 pixels, and according to our method, the process of accessing the pairs of pixels in each frame will be done in a vertical zigzag form, which starts from the upper left corner of the frame, and we walk in the form of a zigzag perpendicular to all the columns of the frame until the message is ended. As shown in Fig. 6 , 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 11 percent in a colored point. All this will be explained in the following algorithms:

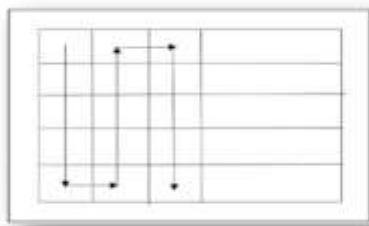


FIG.6: THE TWO-PIXEL BLOCKS THAT DO NOT OVERLAP ARE CREATED BY ZIGZAG SCANNING THE COLUMNS BY ACCUMULATING EVERY TWO PIXELS IN A COVER PICTURE

Algorithm (1): Embedding Algorithm in first method

Input: The selected frame, encrypted secret message in binary

Output: Stego-video

Process:

Step 1: For each selected frame

Step 2: Divide the frame into blocks and on the basis of a vertical zigzag and using secret key $(n+15)$ and thus this key will determine which locations will be used to hide message in the frame.

Step 3: After determining the pixels that will be hidden inside then we will 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 4 : Calculate the difference between the each 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 5: Calculate the new difference value for the pair of pixels and new pixels value

Step 6: 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 7: End for

Step 8: Collected all frames to recreate the stego-video

End.

- 2- **The second method:** applying the MapReduce method on selected frame. This frame will be entered in the MapReduce stages for the purpose of dividing it and controlling it. As a first step, the master will divide the frame into three matrices, which are the (red, green, and blue) matrices, and then each matrix will be sent to the map stage of the MapReduce. Map will perform calculations to give the dimensions of the matrix in terms of width and height and send the result to the next phase which is shuffle and sort phase, the process of hiding the data in the matrix will be done by using the steganography technique, which is the (LSB) technology. In addition, the secret key (x^2) will be used, this will be used to decide the locations of the pixels that will be employed to hide the secret message inside it, and this key will take the shape of the curve as seen

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

in Fig. (7). Then Reduce stage will compile the results of the matrices and display the final frame that has been hidden by it, which is the stego frame.

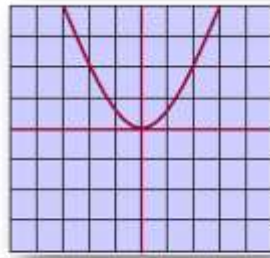


FIG. 7: THE SECRET KEY (x^2) WHICH IS IN THE FORM OF CURVE

Algorithm (2): Embedding Algorithm in second method

Input: The selected frame, encrypted secret message in binary

Output: Stego-video

Process:

Step 1: For each selected frame

Step 2: divide the frame into three matrix, which is the (red, green, and blue) matrices, and then each matrix will be sent to the map stage of the MapReduce.

Step 3: Map will perform calculations to give the dimensions of each matrix.

Step 4: shuffle and sort will use the secret key (x^2) to specify the position of pixel to hide in it and apply the LSB algorithm to hide the message

Step 5: The reducer collect the result of matrixes and generate stego frame

Step 6: End for

Step 7: Collecting all frames to recreate the stego-video

End.

- 3- The third method:** applying the MapReduce method on selected frame. But in this method the master node will divide the frame into four blocks, each block will be sent to MAP so that each MAP makes calculations on the dimensions of the frame block and sends the results to the next stages, which are the shuffle and sort, which in turn will implement the process of hiding the secret message using the technique of (PVD) on each block of the frame separately with using secret key ($n+15$) for the same purpose as explained in the first method. In addition, the hiding process will be carried out on all color channels, thus achieving a high capacity of hiding. The process of dividing the frame is illustrated in Fig. (8). Finally reduce stage will compile the results of the parts and display the stego frame.



FIG.8: THE PROCESS OF DIVIDING THE FRAME INTO FOUR PARTS

Algorithm (3): Embedding Algorithm in third method

Input: The selected frame, encrypted secret message in binary

Output: Stego-video

Process:

Step 1: For each selected frame

Step 2: divide the frame into four block each block send to one map

Step 3: Map will divide the block into three matrix (red ,green ,blue) in order to hide in all color channels and execute computation to generate dimension about the block.

Step 4: shuffle and sort will apply the PVD technique to hide the secret message in each three matrix in a block with the use of the secret key $(n+15)$ to specify the position of pixel

Step 5: The reducer collect the result of blocks and generate stego frame

Step 6: End for

Step 7: Collect all frames to recreate the stego-video

End.

II. Extraction Algorithm

The extracting algorithm is similar to the embedding algorithm but in reverse. It also includes several steps.

- **First step (in each three proposed method):** read the stego video file (it is the video that contains the secret encrypted message) then convert this video into a number of sequential frames in PNG file format.
- **Second step (in each three proposed method):** Select one stego frame from a sequence of frames and also the frame selection process takes place in the same pattern that was previously explained in embedding algorithm. This means we will continue to take the stego frame until the message is completely extracted.
- **Third step:** this step is different according to the method in the first proposed method in applying the inverse (PVD) method on the selected stego frame in order to extract the encrypted secret message. In the second one the stego frame will enter to MapReduce stages, which are Map, Shuffle and Sort and Reduce stage for dividing the frame into three matrix, then applying the inverse LSB in second stage on each matrix. In the last one, also apply MapReduce for the purpose of

Received 22/4/2021; Accepted 25/6/2021

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

dividing the frame, and then in the Shuffle and Sort, apply the inverse (PVD), as for Reducer, it will collect the message from each part to obtain the original secret message.

- **Finally:** converting the binary secret message into ASCII code then to byte code then applying the inverse AES algorithm in order to decrypt the secret message.

VII. EVALUATION OF THE RESULTS

In this section, the results obtained in the three proposed methods will be discussed. These methods aim to hide the confidential message inside a video after encoding it using (AES) to achieve high security. In addition, the MapReduce principle has been used for the purpose of facilitating dealing with video frames in terms of dividing, analyzing and controlling them. These results were examined on a 30-second video with 25 fps and this video is in (mp4) format. This video contains 256 frames. Each frame size is (1280 * 720 pixels).

Table 1 shows the size of several confidential messages and the number of frames taken by each secret message. In addition, it shows the time of encoding and decoding the secret message and the time of including and extracting it for each of the three methods.

TABLE 1. INDICATES THE SIZE OF MESSAGE, NO. OF FRAMES, TIME OF ENCODING DECODING EMBEDDING AND EXTRACTING.













Name of video	Proposed method	Message size	No. of frames	Time of encoding (Second)	Time of decoding (Second)	Time of Embedding (Second)	Time of extracting (Second)
Vid.mp4	First method	12400 Bit	2 frame	0.0473001	0.0	3.0454187	1.5773165
		24790 Bit	4 frame	0.0631043	0.0156211	5.4216139	3.8116033
		37192 Bit	5 frame	0.0781877	0.0156269	8.2010860	4.2333388
	Second method	12400 Bit	7 frame	0.0473001	0.0	0.8278586	2.4681317
		24790 Bit	14 frame	0.0631043	0.0156211	1.6867060	4.4984891
		37192 Bit	21 frame	0.0781877	0.0156269	4.3894228	6.5609562
	Third method	12400 Bit	1 frame	0.0473001	0.0	2.3275527	1.2340857
		24790 Bit	1 frame	0.0631043	0.0156211	4.9989840	2.2650456
		37192 Bit	2 frame	0.0781877	0.0156269	7.2325110	3.9522202

The results obtained in Table\ show the number of frames that were used to hide inside them according to the size of the message, so it has been noted that the second method used the most number of frames, and therefore the capacity is less compared to other methods, because in the message of size (37192 Bit) the second method took (21) frames, while the first method took (5) frames, and the third took (2) frames.

In addition, it was concluded that the embedding time for the first method is the most compared to other methods. In the message size (37192 Bit), the first method took (8.2010860 seconds) while the second method took (4.3894228 seconds) and the third (7.2325110 seconds). As for the time of extraction, it could be concluded that the third method takes the shortest time compared to other methods. In the size of the message (37192 Bit), the first method took (4.2333388 seconds), while the second method took (6.5609562 seconds) and the third method (3.9522202 seconds), so the third method is the fastest method to extract the secret message.







To measure the efficiency of performance of the proposed methods, several measurements were used which are: PSNR, MSE, Entropy, and correlation coefficient; and they will be explained in the following tables. In each table, samples will be taken from the original and stego frames and their results will be presented. Table \ shows the results of the first method.

TABLE 2. INDICATES FOR MEASUREMENTS OF PSNR, MSE, ENTROPY, CORRELATION COEFFICIENT FOR THE FIRST METHOD.

Message size	No. of frames	Name of video frame	Original video frame	Stego- video frame)	PSNR (dB)	MSE	Entropy For original (O) & stego (S) frame	Correlation coefficient
12400 Bit	2 frame	44			68.59609	0.00898	O =7.4556 S =7.4557	0.9975
		54			72.63562	0.00354	O =7.2536 S =7.2536	0.9847
24790 Bit	4 frame (We will only take two frames to show their results)	44			68.41410	0.00936	O =7.4556 S =7.4557	0.9988
		64			69.61890	0.00709	O =7.2309 S =7.2309	0.9850
37192 Bit	5 frame (We will only take two frames to show their results)	74			69.49672	0.00730	O =7.1995 S =7.1996	0.9810
		84			71.45536	0.00465	O =7.3654 S =7.3654	0.9964

It is noticed that the first method in the above table gave good results relative to (PSNR) values ranging from (68.41410 dB) to (72.63562dB) and low values of (MSE). As for the entropy, which measures the distribution of pixels in the frame, it has been noticed that there are no differences and thus image quality was not affected. Moreover, with the correlation coefficient, which measures the degree of correlation of the pixels, the presence of a relative high and low could be noticed in them, but they remain within the acceptable ratio, which is between (0) and (1) and all this proves that this method achieves high accuracy, quality and transparency.









TABLE 3. INDICATES FOR MEASUREMENTS OF PSNR, MSE, ENTROPY, CORRELATION COEFFICIENT FOR THE SECOND METHOD.

Message size	No. of frames	Name of video frame	Original video frame	Stego- video frame)	PSNR (dB)	MSE	Entropy For original (O) & stego (S) frame	Correlation coefficient
12400 Bit	7 frame (We will only take two frames to show their results)	44			82.10988	0.00040	O =7.4556 S =7.4557	0.9980
		54			82.18514	0.00039	O =7.2536 S =7.2536	0.9818
24790 Bit	14 frame (We will only	144			82.18914	0.00039	O =7.1065 S =7.1065	0.9922

	take two frames to show their results)	154		82.20115	0.00039	O =7.4601 S =7.4601	0.9978
37192 Bit	21 frame (We will only take two frames to show their results)	214		82.39803	0.00037	O =7.7228 S =7.7228	0.9926
		244		86.73819	0.00013	O =7.5060 S =7.5060	0.9991

Table 3 shows very good results for the second method in terms of high (PSNR) values ranging from (82.10988dB) to (86.73819dB) and low (MSE) values. As for the entropy, there are no differences and thus image quality was not affected. And the correlation coefficient, the presence of a relative high and low could be noticed in them, but they remain within the acceptable ratio, and this proves that this method achieves very high accuracy, quality and transparency.

TABLE 4. INDICATES FOR MEASUREMENTS OF PSNR, MSE, ENTROPY, CORRELATION COEFFICIENT FOR THE THIRD METHOD.

Message size	No. of frames	Name of video frame	Original video frame	Stego- video frame)	PSNR	MSE	Entropy For original (O) & stego (S) frame	Correlation coefficient
12400 Bit	1 frame	44			66.27152	0.01534	O =7.4556 S =7.4558	0.9982
24790 Bit	1 frame	44			63.50710	0.02899	O =7.4556 S =7.4559	0.9985
37192 Bit	2 frame	44			62.93398	0.03308	O =7.4556 S =7.4559	0.9972
		54			68.97724	0.00822	O =7.2536 S =7.2536	0.9830

It is also noticed in Table 4 good results relative to good (PSNR) values ranging from(62.93398dB) to (68.97724dB) and low values of (MSE). As for the entropy, there are very small differences and that did not affect the quality of the image. And the correlation coefficient, the presence of a relative high and low could be noticed in them, and this proves that this method also achieves very high accuracy, quality and transparency.

TABLE 5. INDICATES COMPARISON RESULTS

Proposed method	Tools	Steganography technique	Color channel	security	result
First method	Use video for the purpose of concealment	PVD	Blue channel	AES	This method took the longest time for modulation, but it also achieves high capacity and high security
Second method	Using the video for the purpose of masking, as well as using the principle of MapReduce for	LSB	RGB channel	AES	Less capacity, so need a larger video if the secret message is longer, high

	the purpose of dealing with video frames				security, high speed
Third method	Using the video for the purpose of masking, as well as using the principle of MapReduce for the purpose of dealing with video frames	PVD	RGB channel	AES	High capacity, It can hide a large size of secret message in a short video, high security, Good speed

In Table 6, the comparisons of three proposed methods with previous works are done to show the differences in techniques, tools, color channel and security. The three proposed methods are more robust than the previous work in refs. [7], [12], [18] and [34]. In terms of (PSNR), (MSE) in bold font, and security, because the AES algorithm was used to encrypt the secret message in three proposed methods, whereas previous works did not use any encryption algorithm.

TABLE 6. INDICATES COMPARISON RESULTS WITH OTHER WORKS.

References	Tools	Steganography technique	Color channel	security	PSNR	MSE
proposed method 1	Use video for the purpose of concealment	Non-overlapping PVD	Blue channel	AES	72.6356 dB	0.00354
proposed method 2	Use video for the purpose of concealment and MapReduce method	LSB	RGB channel	AES	86.7381 dB	0.00013
proposed method 3	Use video for the purpose of concealment and MapReduce method	Non-overlapping PVD	RGB channel	AES	68.9772 dB	0.00822
Ref.[7]	Using image	LSB	Blue and green	Non	55.6750 dB	0.2111
Ref.[12]	Using image	LSB and secret map techniques	RGB channel	Non	45.8661 dB	1.1174
Ref.[18]	Using image	PVD and modulo operation	RGB channel	Non	37.87 dB	---
Ref.[34]	Using image	Overlapping PVD	RGB channel	Non	35.66 dB	---

VIII. CONCLUSION

The proposed methods aim to achieve complete secrecy in the transfer of confidential data from one party to another, by hiding this data in a video using the techniques of concealment (PVD) and (LSB) according to the method. Because the video is the effective way that can be used as a carrier media. So hiding data in video streams and frames play an important role in steganography and the concept of MapReduce programming model is used in this paper in order to facilitate dealing with the video frames as a big data in terms of dividing, analyzing and controlling them. In addition to that, the message was encrypted using the (AES) algorithm. The results of this system are efficiency, transparency, robustness, powerful in stego video, high capacity, and high security. The attacker or unauthorized person cannot detect any suspicious differences in a stego video.

REFERENCES

- [1] I. A. T. Hashem, N. B. Anuar, A. Gani, I. Yaqoob, F. Xia and S. U. Khan, "MapReduce: A bibliometric, review and open challenges", pp.1-35,2016.
- [2] S. Maitreya and C.K. Jha, "MapReduce: Simplified Data Analysis of Big Data", *rocedia Computer Science* 57, pp. 563 – 571, 2015.
- [3] X. Li, J. Song, F. Zhang, X. Ouyang, and S. U. Khan, "MapReduce-based fast fuzzy c-means algorithm for large-scale underwater image segmentation", *Future Generation Computer Systems*, vol. 65., pp. 90–101, 2016.
- [4] I. A. T. Hashem, "MapReduce scheduling algorithms: a review", *The Journal of Supercomputing* 76(7), pp. 4915–4945, 2020.
- [5] S. N. Khezr and N. J. Navimipour, "MapReduce and Its Applications, Challenges, and Architecture: a Comprehensive Review and Directions for Future Research", *Journal of Grid Computing*, vol. 15, no. 3, pp. 295–321, 2017.
- [6] Gursukhmani and S. Sharma, "Case Study of Hiding a Text Using Video Steganography", *International Journal of Scientific & Engineering Research* Volume 8, Issue 5, pp.1849-1853, 2017.
- [7] Emam, Marwa M., Abdelmgeid A. Aly, and Fatma A. Omara. "An improved image steganography method based on LSB technique with random pixel selection." *International Journal of Advanced Computer Science and Applications* 7.3, pp. 361-366, 2016.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] A. K. H. Al-Saedi, "A method to hide text in image", *Journal of Missan Researches*, vol. 12, no. 24., pp. 11–23.2016.
- [12] A. Alabaichi, Maisa'a. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques", *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1. pp. 935–946, 2020.
- [13] G. P. Rajkumar and V. S. Malemath, "Video Steganography: Secure Data Hiding Technique", *I. J. Computer Network and Information Security*, pp: 38-45, 2017.
- [14] N. Manohar and P. V. Kumar, "Data Encryption Decryption Using Steganography", *Proceedings of the International Conference on Intelligent Computing and Control Systems, ICICCS*, pp. 697–702, 2020.
- [15] D. Hasibuan and J. Napitupulu, "Pixel Value Differencing Algorithm in Steganography Image", *International Journal of Recent Trends in Engineering & Research (IJRTER)* Volume 03, Issue 04; [ISSN: 2455-1457], pp: 98-101, 2017.
- [16] M. A. hameed, Hassaballah, S. Aly and A. S. A. Rady, "A High Payload Steganography Method based on Pixel Value Differencing", *Informatics and Systems*, 2018.
- [17] 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.
- [18] A. K. Sahu and G. Swain, "Digital Image Steganography using PVD and Modulo Operation", *INTERNETWORKING INDONESIA JOURNAL*, ISSN: 1942-9703 / CC BY-NC-ND, pp. 3-13, 2018.
- [19] M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. S. Reddy and M. Venkatesh, "Digital Video Steganography Using LSB Technique", *IRE Journals*, Volume 3 Issue 10, pp.14-17, 2020.
- [20] K. B. Sudeepa, K. Raju, H. S. Ranjan Kumar, and G. Aithal, "A New Approach for Video Steganography Based on Randomization and Parallelization", *Physics Procedia*, vol. 78, pp. 483–490, 2016.
- [21] J. Kaur and J. Kaur, "Hiding Text in Video Using Steganographic Technique - A Review", vol. 17, no. January, pp. 578–582, 2016.
- [22] G. Nikam, Ankit Gupta, V. Kalal and P. Waghmare, "A Survey of Video Steganography Techniques", *Journal of Network Communications and Emerging Technologies (JNCET)*, Volume 7, Issue 5, pp. 33-35,2017.
- [23] Deshmukh and B. Rahangdale, "Data Hiding using Video Steganography", *International Journal of Engineering Research & Technology (IJERT)*, Vol. 3 Issue 4, pp.856-860, 2014.
- [24] D. Deshmukh and G. Kurundkar, "Video Steganography using Edge Detection Techniques", *International Conference on Communication and information Processing (ICCIIP-2019)*, pp.1-4,2019.
- [25] 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), pp. 105-108, 2014.
- [26] P. V. Shinde and T. B. Rehman, "A Survey : Video steganography techniques", *International Journal of Engineering Research and General Science* Volume 3, Issue 3, ISSN 2091-2730, pp.1457-1464, 2015.
- [27] A. John and A. Baby, "A Survey on Video Steganography", *International Journal of Science and Research (IJSR)* ISSN: 2319-7064, Volume 8 Issue 4, pp. 800-805, 2019.
- [28] H. M. Ahmed and Maisa'a. A. A. K. Al-Dabbas, "Arabic Language Text Steganography Based on Singular Value Decomposition (SVD)", *Eng. &Tech.Journal*, Vol.34,Part (B), No.5, pp. 629–637,2016.

DOI: <https://doi.org/10.33103/uot.ijccce.21.2.9>

- [29] A. Moneem S. Rahma and Maisa'a. A. A. Khodher, "Proposed Method for Partial Audio Cryptography Using Haar Wavelet Transform", IJCCCE Vol.13, No.2, pp. 11–18 , 2013.
- [30] A. Moneem S. Rahma and Maisa'a. A. A. Khodher., "To Modify the Partial Audio Cryptography for Haar Wavelet Transform by Using AES Algorithm", Eng. & Tech. Journal, Vol.32, Part (B), No.1, pp. 169–182, 2014.
- [31] Maisa'a. A. A. K. Al-Dabbas, A. Alabaichi, and A. S. Abbas,"Dual method cryptography image by two force secure and steganography secret message in IoT", *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6., pp. 2928–2938, 2020.
- [32] Maisa'a. A. A. Khodher and Teaba W. A. Khairi," Review: A comparison Steganography Between Texts and Images", *Journal of Physics: Conference Series* 1591 , pp. 1–8, 2020 .
- [33] A. Malik, G. Sikka, and H. Kumar Verma, "A Modified Pixel-Value Differencing Image Steganographic Scheme with Least Significant Bit Substitution Method", *International Journal of Image, Graphics and Signal Processing*, vol. 7, no. 4. pp. 68–74, 2015.
- [34] R. T. Sabbah, " A Comparable study of hiding information in images using least significant bit (LSB) substitution and pixel value difference (PVD) Method", PhD Thesis, 2016.
- [35] M. Hussain, A. W. Abdul Wahab, N. Anuar, R. Salleh and R. Md Noor," Pixel Value Differencing Steganography Techniques: Analysis and Open Challenge", *IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, 2015.
- [36] E. M. El-Alfy and A. A. Al-Sadi, "Pixel-Value Differencing Steganography: Attacks and Improvements", *ICCIT*, pp. 757-762, 2012.
- [37] 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.
- [38] Jung and Ki-Hyun. "Data hiding scheme based on pixel-value differencing in dual images." *International Conference on Electronics, Information, and Communication (ICEIC)*. IEEE, 2018.
- [39] S. Prasad and A. K. Pal, "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing", *royal society open science*, pp:1-14 , 2017.
- [40] S. N. Khezr and N. J. Navimipour, "MapReduce and Its Application in Optimization Algorithms: A Comprehensive Study", *Majlesi Journal of Multimedia Processing* Vol. 4, No. 3, pp. 29-33 , 2015
- [41] A. Elsayed, O. Ismail, and M. E. El-Sharkawi, "MapReduce: State-of-the-Art and Research Directions", *International Journal of Computer and Electrical Engineering*, pp. 34–39, 2014.
- [42] J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters", *OSDI*, pp. 1-13, 2004.