Using the principle of mapreduce for steganography to hide the encrypted message in video based on pvd method

Huda Ghazie Abd UL Sahib[1,a)], Maisa'a Abid Ali Khodher [2,b)]

[1,2]Department of computer sciences, University of Technology, Baghdad, Iraq

[a)] cs.19.03@grad.uotechnology.edu.iq
[b)] 110044@uotechnology.edu.iq

Published online 28-11-2022

Abstract. Continuous increases in computing ability have produced overwhelming data or big data flow over recent years, which exceeds the capabilities of traditional processing tools. Therefor the processing and analysis of this big data is become a challenge, and also must provide secure transmitions of these data for that reason must understand how to deal with the complexity of the data and their requirement about how to partition the tasks and executed them in a parallel and how to protect these data in order to prevent the attacker, intruder and unauthorized person to access to the important information.

The proposed system is convert the original video in to a sequence of frames then hiding the secret message into these frames after encrypted it by using one of stronger encryption algorithm AES. The system consists of many phases: firstly, divided video in many frames, after that the frame that selected for hide the secret message in it is inserted to MapReduce phases, this frame is input to master node that divided it into four blocks, then send each block to mapper each block is divided into three matrix (red, green, blue) , a mapper will execute some computation to generate intermediate result and send the result to shuffle and sort phase, in this phase the processing of hiding the secret message will done by using the pixel value difference (PVD) method with use the secret key (n+15) this key will determined the position that will take to hide the secret message in it. Finally, the shuffle and sort send the result of each block to the reducer, the reducer will collect these result to generate the stego-frame. The results of this system is efficiency, transparency, robustness, powerful in stego video , high capacity , and high security the attacker or unauthorized person cannot detected any suspicious differences in a stego video. This results is obtained through use many measurements PSNR, MSE, Entropy, correlation coefficient.

Keywords. Steganography, AES, PVD, MapReduce, Secret key.

1. INTRODUCTION

Big data has emerged as a research field in the digital knowledge interval to accurately tackle the vast quantities of data generated. Traditionally, this data involves vast quantities of data formats that are unstructured. Scientifically, these data are exceedingly complex for storage, processing and study using conventional bases of data [1]. A large amount of hard work is needed in solving a big dataset problem. An interpretation of such big data, however, is a very difficult issue today [2]. Parallel computing paradigms like the MapReduce system have been proven as a viable solution to deal with this issue [3]. Recently, the MapReduce system has been very interesting for such an application that operates on extensive data [4]. The 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 confidential 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 is also necessary, data security means securing a data from harmful powers and unauthorized users' discarded acts [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 applies to encoding procedure of confidential data such that only the right person with the right key can successfully decode and retrieve the original data [7]. DES, AES, RSA and other are the most common encryption techniques [8]. Another way is data hiding, hiding data is the method of injecting information without causing perceptual degradation into media files. Two popular techniques in data hiding can be used. It is steganography and watermarking [9].

Steganography is characterized as the art and knowledge of writing secret messages so that nobody knows the existence of a message other than the intended recipient. The term 'steganography' literally comes from Greek and means 'hidden writing.' The word is divided into two sections: steganos meaning "secret" and "graphic," meaning "writing."[10]. Steganography must satisfy the basic requirement 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 classify as a spatial domain or a frequency domain. Frequency domain means transforming images into frequency components through a discrete cosine transform, fast Fourier transform and discrete wavelet transform (DWT). In the spatial domain, Depending on the intensity of the pixels, information is concealed directly. Frequency domain methods are stable, mostly used for watermarking, while approaches of spatial domain deliver high capacity and are commonly used in steganography [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 relevant 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].

This paper will use the video steganography, video steganography 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 it is much important to protect our data or information from intruder and hackers or unwanted access [14].

2. RELATED WORK

There is a lot of studies and researches that includes the topics of dealing with big data and how to provide a security to these data in this paper will take the MapReduce system that demonstrates how to dealing with and processing big data and take the researches about the steganography technique that hiding 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 was 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 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 explores 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 conclude from their research The Pixel Value 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), Mohamed Abdel hameed and et.al. Their paper proposed a PVD-based approach called adaptive horizontal and diagonal pixel values difference method (A-HDPVD) for secret hiding Data in the picture coverage RGB channels. The approach employed by A-HDPVD enhanced the original PVD algorithm to adaptively choose different directions (horizontal and diagonal) for each color of the embedded channel. The A-HDPVD method serves to enhance the payload for embedding and reasonable image quality. And they conclude that The PSNR value of a diagonal direction is greater than the other direction of the image. Relative to the other horizontal direction, the diagonal direction has the largest embedding payload [16].

In (2018), P. Srilakshmi and et.al. Their paper proposed new method to image steganography for the spatial domain embedding of text. The message is dumped into the image in the suggested input with reference to a randomly generated key, 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 present an image steganography method by use 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 using two phases, (1) pixel difference modulo operation (PDMO) phase, and (2) average PVD (APVD) phase of readjustment. First, the differences between a block's consecutive pixels are identified then the hidden data are embedded by modulo operation and adaptive range table. For 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 research carried out in the field of planning on big data platforms. This paper examined preparation on two aspects in MapReduce: taxonomy and performance assessment. Their 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].

3. VIDEO STEGANOGRAPHY

Video steganography is a relatively new steganographic medium, there have been some interesting schemes proposed which encode information in multiple domains of video sequences [20]. In real life, Video Steganography is a very critical activity in which users want data confidentiality [21].

Video steganography is a way to conceal data or information in video format frames. Various methods are used to hide the secret data in various video frames safe from the human eye [22]. The video file can conceal significant quantities of information because it contains several frames and also has more storage space and can conceal more detail than the audio and image files [23].

Digital video is a series of frames that play at a fixed frame rate. The frame rate depends on the regular video. Digital video Quality depends on parameters such as fps, the amount of pixels in a frame and the size of a frame. 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 [24] [25][26].

Three forms of images exist (or frames) used to test the frames video compression: I-frames, P-frames and B-frames specified for compression of data [27]. They have distinct characteristics: I (Intra-coded) frames do not need to decode other video frames but are less compressible. P-(Predicted) frames uses information from previous frames to decompress and are more compressible than I frames. The B- (Bi-predictive) frames are used previous and forward Data reference frames for higher data compression [26][28][29].

The benefit of using video as a cover medium for data storage is that the data can be stored in large spaces. More protection is provided against the attacker because the video file is much more complex than the image file. One Another benefit is that the hidden data are not known by the human eye is insignificant as the pixel color varies [27][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 hidden 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. 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 insertion technique is developed in PYTHON. The video steganography block diagram is seen in the Fig .1.

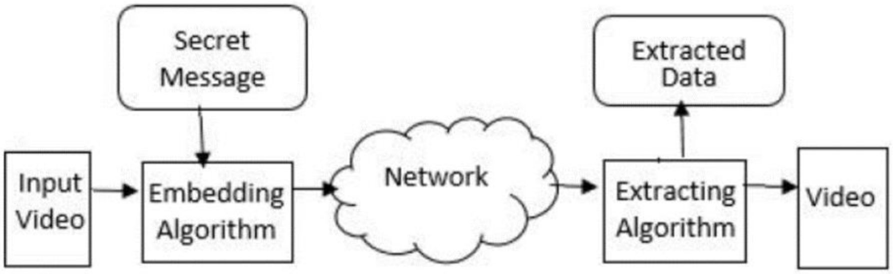

Fig. 1: The video steganography block diagram

4. PIXEL VALUE DIFFERENCE ALGORITHM (PVD)

Pixel value difference is a method of steganography, it is suggested by Wu and Tsai 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]. Originally, the Pixel Value Differencing (PVD) approach was proposed to conceal hidden messages in 256 gray value of images. It can add vast volumes of data without any harm to the image quality, therefore human eyes hardly notice them. PVD uses the difference between each pair of pixels to decide the number of message bits to be inserted in that pair of pixels [36].
At first the image is partition into blocks that do not overlap by two consecutive pixels, p_i and p_{i+1} [8] .the way of partition run through all rows to each image it begins at the upper left corner of the cover image and scanning it in a zigzag manner as seen in the Fig. 2.[36][37]

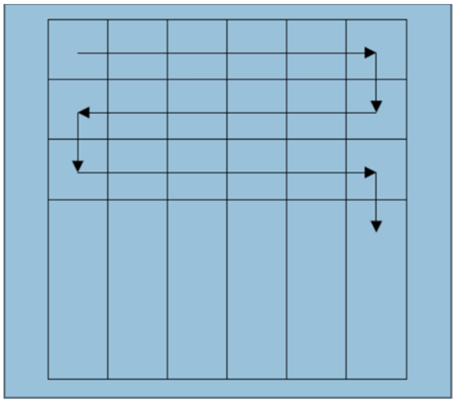

Fig. 2: The PVD non-overlapping two-pixel blocks are created by zigzag
Scanning the rows in a cover image

The differential value d_i is determined from each block via subtracting pi 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. The eyes can handle more sharp edge changes than the smooth areas, according to the properties of human vision. 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. 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].
In a proposed method will use R = {[0.7], [8.15], [16.31] [32.63], [64.127], [128.255]}, 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]:

$$\text{Number of bit} = Log_2\,(\text{upper width-lower width+1})$$

OR by n = number of bit

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

The series of bits obtained is transformed to decimal value then new difference value is calculated using the equation: di'=lower width+b OR by

di'=2^n+b but if $0 <= di < 8$ *then* $di' = b$

The adjusted pixel values are determined on the basis of the following condition:

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

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' – lower i) OR by secret bit = (di' –2^n) but if 0<= di' <8 the secret bit = di' [39].

The PVD have some limitation this limitation is fall boundary issues [18] that's mean 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.

5. MAP REDUCE

The excessive increase in knowledge and data now makes their analysis a burdensome challenge [40], new techniques in software, hardware and algorithms are required to meet the demands for analysis of ever-growing data [41]. Number of parallel algorithms was 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 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 application writing that can process Big Data on multiple nodes in parallel. MapReduce offers analytical ability to evaluate vast quantities of complicated data [42]. MapReduce is designed for programmers instead of business users. It's a 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. It also has the advantage that developers do not struggle with parallel processing the device is done transparently [2].

The basic architecture of MapReduce as the following:

MapReduce operates in a node cluster; one node functions like as a master node and other nodes feature act as workers. Nodes of workers are responsible for map and reduce tasks running [41]; and the main three components of MapReduce is: 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 is:

- Input step (master) − The master is responsible for maintaining and providing data and procedures for map and reduce functions 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 processes input data that the master assigns for computation and it generates the output in the form of a pair of key/value item.
- 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 figure below.

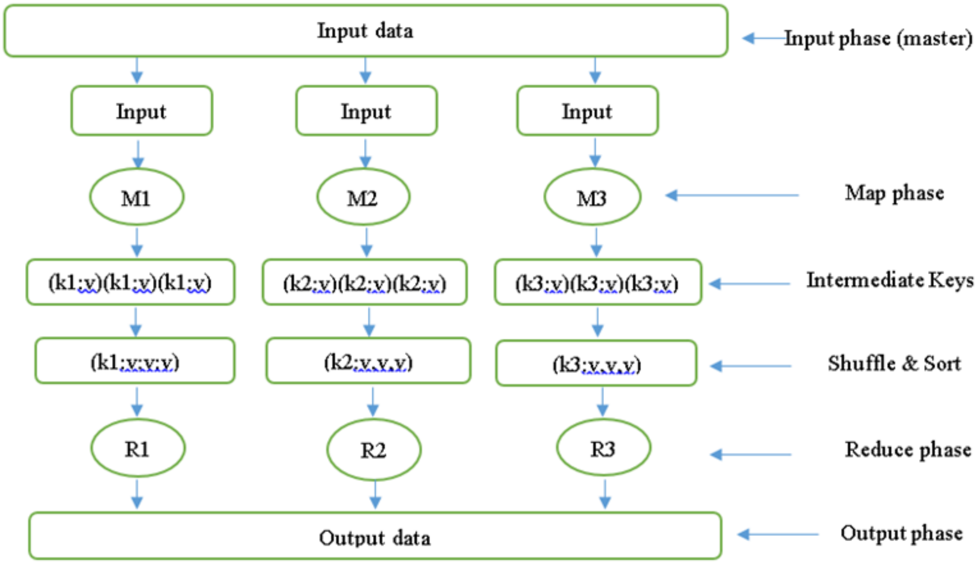

Fig.3: the basic architecture of MapReduce

MapReduce is used in many applications for massive data [41], it is used in optimization algorithm such as genetic algorithm and Ant colony algorithm and so on [40], and also it is used in another application such as URL frequency count: 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 [42].

Another popular example is 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 a proposed method will use the mapreduce algorithm for steganography to deal with hiding encrypted secret and confidential message in a video by using many steps because the video is providing a big size to conceal a large amount of data.

6. PROPOSED METHOD

Due to the development of computer and communication technologies, there is enormous increase in the growth of data, therefore must provide a technique in order to be able for dealing with this enormous data and information and also when the need to transfer this data over the internet, therefore, there must be a good way to protect this important data from unauthorized users or attackers who want access to these sensitive data.

So in the proposed method will used MapReduce algorithm for steganography to hide the encrypted message in video based on PVD steganography technique because the video is a powerful means of concealment. And can hide a large amount of data without being noticed by the human eye or by attackers.

First of all the original video is converting into sequence of frame in order to hide the secret message in it after encrypted this secret message by using (AES) encryption algorithm but the proposed method will not use all frames, it is used one frame out of every ten shots of frames, each frame will be included in the phases of MapReduce as follows, send one frame to the master node the master will divided the frame into four block.

Then each block is send to worker, the workers are responsible for execute the map and reduce task.in a mapper the block is divided in to three matrix (red, green, blue) and execute some computation to generate the intermediate result about the matrix dimensions. These result is send to the next phase it is shuffle and sort phase this phase is take a result from the previous phase and use it to apply the pixel value difference (PVD) method in order to conceal the encrypted secret message in a block with a secret key (n+15) this key will determined the position of the pixels that will uses to hide the secret message. Finally the shuffle and sort send the result of each block to the reducer, the reducer will collect these result to generate the stego frame.

There are two algorithms that must follow in our proposed method the first algorithm is embedding and the other one is extracting algorithm as will illustrate them in the diagrams below:

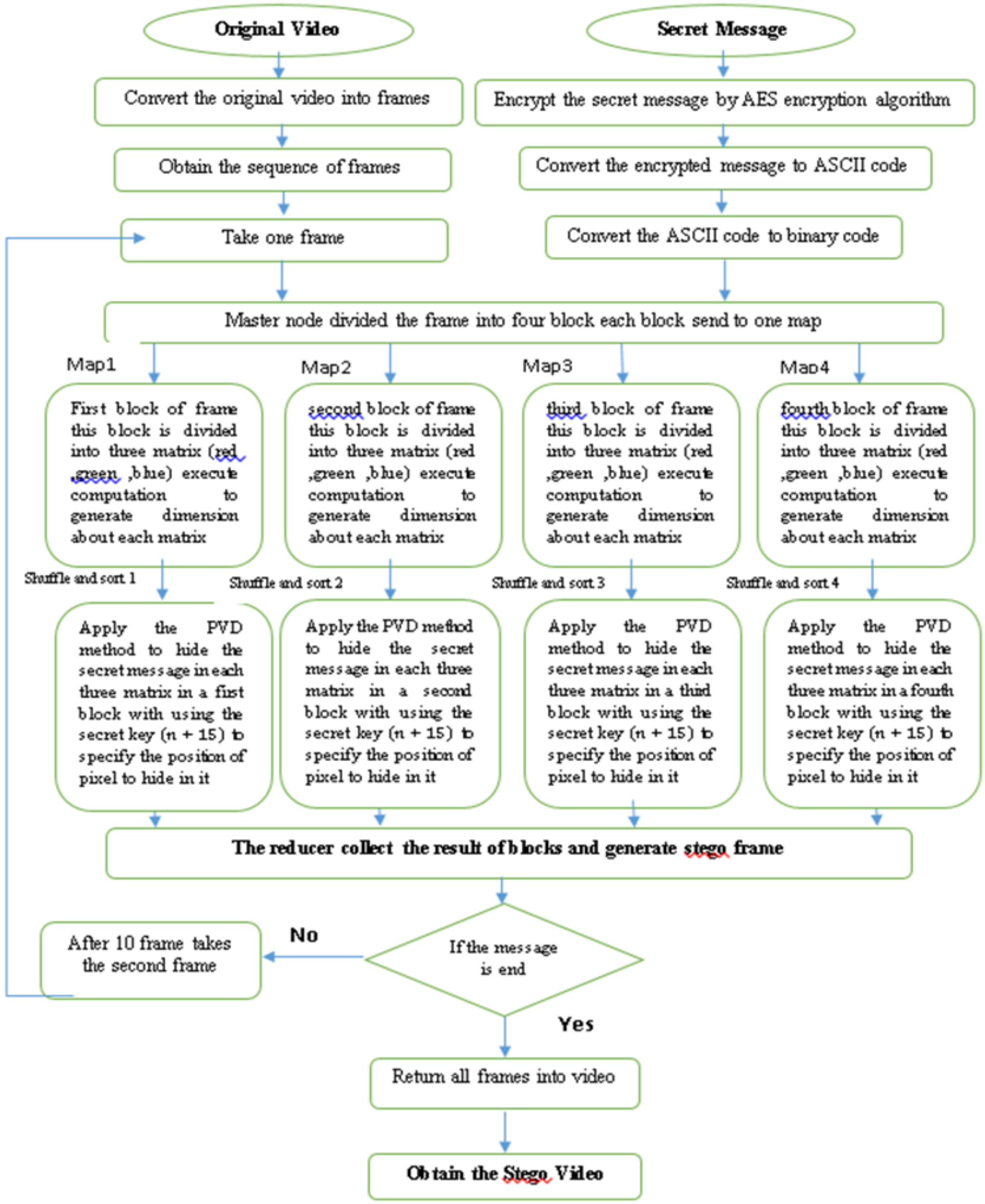
Original Video
Secret Message
Convert the original video into frames
Encrypt the secret message by AES encryption algorithm
Obtain the sequence of frames
Convert the encrypted message to ASCII code
Take one frame
Convert the ASCII code to binary code
Master node divided the frame into four block each block send to one map
Map1
Map2
Map3
Map4
First block of frame this block is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
second block of frame this block is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
third block of frame this block is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
fourth block of frame this block is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
Shuffle and sort 1
Shuffle and sort 2
Shuffle and sort 3
Shuffle and sort 4
Apply the PVD method to hide the secret message in each three matrix in a first block with using the secret key (n + 15) to specify the position of pixel to hide in it
Apply the PVD method to hide the secret message in each three matrix in a second block with using the secret key (n + 15) to specify the position of pixel to hide in it
Apply the PVD method to hide the secret message in each three matrix in a third block with using the secret key (n + 15) to specify the position of pixel to hide in it
Apply the PVD method to hide the secret message in each three matrix in a fourth block with using the secret key (n + 15) to specify the position of pixel to hide in it
The reducer collect the result of blocks and generate stego frame
If the message is end
No
After 10 frame takes the second frame
Yes
Return all frames into video
Obtain the Stego Video

Fig. 4: The flowchart diagram of embedding algorithm

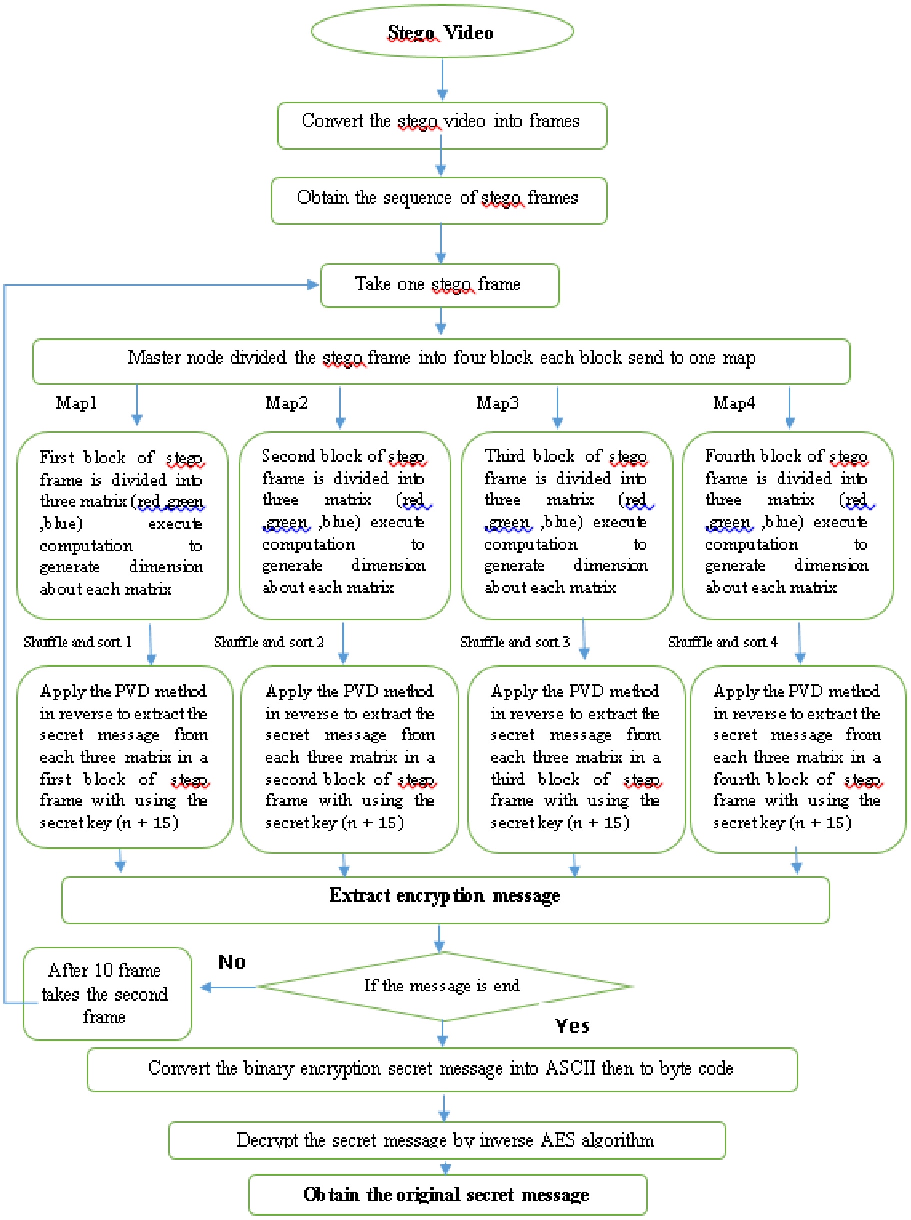
Stego Video
Convert the stego video into frames
Obtain the sequence of stego frames
Take one stego frame
Master node divided the stego frame into four block each block send to one map
Map1
Map2
Map3
Map4
First block of stego frame is divided into three matrix (red,green ,blue) execute computation to generate dimension about each matrix
Second block of stego frame is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
Third block of stego frame is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
Fourth block of stego frame is divided into three matrix (red ,green ,blue) execute computation to generate dimension about each matrix
Shuffle and sort 1
Shuffle and sort 2
Shuffle and sort 3
Shuffle and sort 4
Apply the PVD method in reverse to extract the secret message from each three matrix in a first block of stego frame with using the secret key (n + 15)
Apply the PVD method in reverse to extract the secret message from each three matrix in a second block of stego frame with using the secret key (n + 15)
Apply the PVD method in reverse to extract the secret message from each three matrix in a third block of stego frame with using the secret key (n + 15)
Apply the PVD method in reverse to extract the secret message from each three matrix in a fourth block of stego frame with using the secret key (n + 15)
Extract encryption message
After 10 frame takes the second frame
No
If the message is end
Yes
Convert the binary encryption secret message into ASCII then to byte code
Decrypt the secret message by inverse AES algorithm
Obtain the original secret message

Fig. 5: The flowchart diagram of extracting algorithm

6.1. EMBEDDING ALGORITHM

1- Take the secret message and encrypt it by using AES encryption method and convert this encryption message into byte code then convert it into ASCII code finally into binary code.
2- Take the original video and divided it into sequence of frames, the video is a powerful means of concealment. It can hide a large amount of data without being noticed by the human eye or by attackers.
3- Distribute the encrypted message on the frames. But not take all frame of video in sequence manner in this method will take one frame out of every ten shots of frames.
4- send one frame to the master node the master will divided the frame into four block
5- Then each block is send to worker, the workers are responsible for execute the map and reduce task.
6- In the map phase each mapper will divided the block into three matrix (red,green,blue) and execute some computation to generate the intermediate result about the matrix dimensions and send the result to shuffle and sort phase.

7- In a shuffle and sort phase use the dimensions of the matrix and start to apply the pixel value difference (PVD) algorithm.
8- The (PVD) algorithm is start by divided each matrix into number of non_overlapping blocks each block contain two pixel but these blocks are divided on the basis of the secret key (n+15) and the partition will not be done on the traditional way by all the row for each matrix and moving as a zigzag, but the partition will be done by moving as a zigzag manner of the columns in each matrix ,Therefore it is impossible for the unauthorized parties to find out any hiding operation of big data in the frames. As seen in figure below:

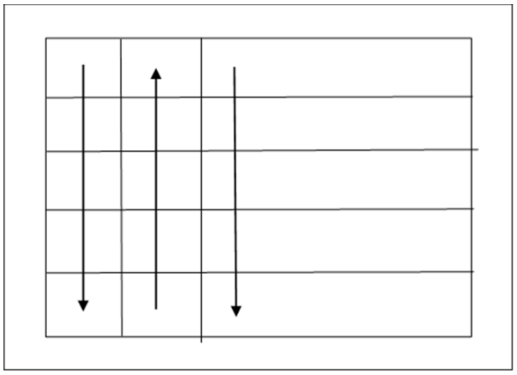

Fig. 6: The PVD non-overlapping two-pixel blocks are created by zigzag Scanning the columns in each matrix

9- Then apply the (PVD) algorithm using the previously explained equations. In addition the proposed method added some adjustments on the method of PVD about exceeding the range (0-255) in the stego frame and remove the drawback of PVD method by not allow to exceed the range (0-255).
10- After the hiding processing is complete the reduce phase is collect the four block to generate the stego frame.
11- Repeat this steps for a number of frames until the message is ending
12- Finally After the message is hidden in a number of frames, must collect all frames together to allow us to create a video again this video is called stego video, this video is the one that will send to the destination.

6.2 . EXTRACTED ALGORITHM

1- Extracting algorithm is the opposite of embedding algorithm, at this point will take the stego video, it is the video that contains the secret encrypted message.
2- Divided the video in to frames.
3- Also take one stego frame out of every ten shots of frames then send the frame to master node. The master will divided the stego frame into four block and send each block to mapper.
4- In the map phase each mapper will divided the block into three matrix (red,green,blue) and execute some computation to generate the intermediate result about the matrix dimensions and send the result to shuffle and sort phase.
5- In shuffle and sort phase apply the algorithm of (PVD) on each matrix in reverse to extract the encrypted secret message.
6- Repeat that steps for all stego frames until all encrypted secret message is extracting.
7- Then converting the binary secret message into ASCII code then to byte code.
8- Finally apply the AES decryption algorithm to obtain the original secret massage.

7. TEST OF THE RESULT

This section discussion the result of proposed system, the system will use the principle of MapReduce algorithm for steganography to deal with hiding encrypted secret and confidential message in a video by using many steps because the video is providing a big size to conceal a large amount of data. And talks from implementation of each frame in video after hide encryption message, as shown in Table 1. And using a set of measurement PSNR, MSE, Entropy, and correlation coefficient. These measurement are explain in Table 2.

• The analysis system in this paper focus on how to dealing with big data and how to processing them in an efficient way to increase the speed of processing by using MapReduce algorithm and also focus how to protect the secret message by encrypted and hiding it in a video after using the (AES) encryption method and (PVD) steganography technique in order the secret message cannot detected by the attacker or unauthorized person.

TABLE 1. Indicates for implementation of stego-frame video.

Name of video frame	Original video frame	Stego- video frame
44		
54		
64		
74		
84		

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

Name of video frame	PSNR	MSE	Entropy	Correlation coefficient
Original video frame(44)	17.9426	71.1448	7.4556	0.9986
Stego- video frame(44)	17.9432	71.1440	7.4559	0.9976
Original video frame(54)	17.4421	38.1532	7.2536	0.9862
Stego- video frame(54)	17.4426	38.1536	7.2536	0.9831
Original video frame(64)	17.4428	37.4726	7.2309	0.9838
Stego- video frame(64)	17.4413	37.4730	7.2309	0.9852
Original video frame(74)	17.4382	36.6935	7.1995	0.9790
Stego- video frame(74)	17.4336	36.6940	7.1996	0.9832
Original video frame(84)	17.4535	43.4215	7.3654	0.9968
Stego- video frame(84)	17.4446	43.4215	7.3655	0.9950

8. CONCLUSION

The concept of MapReduce programing model is used in this paper in order to dealing with the video frames as a big data and used the pixel value difference (PVD) steganography method for hiding the secret message after encrypted it by using AES encryption algorithm . In this paper many measurement 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. Good results have been concluded with relatively high and low in a result of PSNR ranging between (17.4336 and 17.9432), there is a little error ratio and concluded a good result of entropy and correlation coefficient. 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) and hiding (19440) characters in some of these frames. The results of this system is efficiency, transparency, robustness, powerful in stego video , high capacity , and high security the attacker or unauthorized person cannot detected any suspicious differences in a stego video.

REFERENCES

[1] I. A. T. Hashem, N. B. Anuar , A. Gani , I. Yaqoob , F. Xia , S. U. Khan ,2016, MapReduce: A bibliometric, review and open challenges,pp:1-35

[2] S. Maitreya, C.K. Jha, 2015, MapReduce: Simplified Data Analysis of Big Data, rocedia Computer Science 57, pp: 563 – 571

[3] X. Li, J. Song, F. Zhang, X. Ouyang, and S. U. Khan, 2016, MapReduce-based fast fuzzy c-means algorithm for large-scale underwater image segmentation, Future Generation Computer Systems, vol. **65**. pp. 90–101, doi: 10.1016/j.future.2016.03.004.

[4] I. A. T. Hashem, 2020, MapReduce scheduling algorithms: a review, *The Journal of Supercomputing* **76**, pp: 4915–4945,doi.org/10.1007/s11227-018-2719-5

[5] S. N. Khezr and N. J. Navimipour, 2017, 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, doi: 10.1007/s10723-017-9408-0.

[6] Gursukhmani, S. Sharma, 2017, Case Study of Hiding a Text Using Video Steganography, *International Journal of Scientific & Engineering Research* Volume **8**, Issue 5, http://www.ijser.org,pp:1849-1853.

[7] M. M., A. A., and F. A., 2016, 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. , doi: 10.14569/ijacsa.2016.070350.

[8] J. k. Mandal, 2012, 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, doi: 10.5121/ijist.2012.2408.

[9] R. Ibrahim and T. S. Kuan, 2011, Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Application, vol. **2**. pp. 102–108.

[10] V. Sharma and S. Kumar, 2013, 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.

[11] A. K. H. Al-Saedi, 2016, A method to hide text in image, Journal of Missan Researches, vol. **12**, no. 24. pp. 11–23.

[12] A. Alabaichi, Maisa'a. A. A. K. Al-Dabbas, and A. Salih,2020, Image steganography using least significant bit and secret map techniques, *International Journal of Electrical and Computer Engineering*, vol. **10**, no. 1. pp. 935–946, doi: 10.11591/ijece.v10i1.pp935-946.

[13] G. P. Rajkumar, V. S. Malemath, 2017, Video Steganography: Secure Data Hiding Technique, I. J. Computer Network and Information Security, pp: 38-45

[14] N. Manohar and P. V. Kumar, 2020, Data Encryption Decryption Using Steganography, *Proceedings of the International Conference on Intelligent Computing and Control Systems*, ICICCS 2020. pp. 697–702, doi: 10.1109/ICICCS48265.2020.9120935.

[15] D. Hasibuan, J. Napitupulu, 2017, 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

[16] M. A. hameed, Hassaballah, S. Aly, A. S. A. Rady, 2018,A High Payload Steganography Method based on Pixel Value Differencing, Informatics and Systems (INFOS 2018), doi.org/10.1145/nnnnnnn.nnnnnnn.

[17] P. Srilakshmi, C. Himabindu, N. Chaitanya, S. V. Muralidhar, M. V. Sumanth, and K. Vinay, 2018, Text embedding using image steganography in spatial domain, *International Journal of Engineering and Technology (UAE)*, vol. **7**, no. 3. pp. 1–4, doi: 10.14419/ijet.v7i3.6.14922.

[18] A. K. Sahu, G. Swain, 2018, Digital Image Steganography using PVD and Modulo Operation, *INTERNETWORKING INDONESIA JOURNAL*, ISSN: 1942-9703 / CC BY-NC-ND, pp: 3-13

[19] M. V. S. Tarun, K. V. Rao, M. N. Mahesh, N. S. Reddy, , M. Venkatesh,2020, Digital Video Steganography Using LSB Technique, APR 2020 | *IRE Journals* | Volume **3** Issue 10 |, pp:14-17.

[20] K. B. Sudeepa, K. Raju, H. S. Ranjan Kumar, and G. Aithal, 2016, A New Approach for Video Steganography Based on Randomization and Parallelization, *Physics Procedia*, vol. **78**. pp. 483–490, doi: 10.1016/j.procs.2016.02.092.

[21] J. Kaur and J. Kaur, 2016, Hiding Text in Video Using Steganographic Technique - A Review, vol. **17**, no. January. pp. 578–582.

[22] G. Nikam, Ankit Gupta, V. Kalal, P. Waghmare, 2017, A Survey of Video Steganography Techniques, *Journal of Network Communications and Emerging Technologies (JNCET)*, Volume **7**, Issue 5, pp: 33-35

[23] Deshmukh,B. Rahangdale,2014, Data Hiding using Video Steganography, *International Journal of Engineering Research & Technology (IJERT)*, Vol. **3** Issue 4, pp:856-860.

[24] D. Deshmukh,G. Kurundkar ,2019, Video Steganography using Edge Detection Techniques, *International Conference on Communication and information Processing (ICCIP-2019)*, pp:1-4.

[25] K. U. Singh,2014, 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.,

[26] P. V. Shinde, T. B. Rehman,2015,A Survey : Video steganography techniques, *International Journal of Engineering Research and General Science* Volume **3**, Issue 3, ISSN 2091-2730, pp:1457-1464

[27] A. John, A. Baby, 2019, A Survey on Video Steganography, *International Journal of Science and Research (IJSR)* ISSN: 2319-7064, Volume **8** Issue 4, pp: 800-805

[28] Hanaa M. Ahmed, Maisa'a. A. A. K. Al-Dabbas, 2016, Arabic Language Text Steganography Based on Singular Value Decomposition (SVD), *Eng. &Tech.Journal*, Vol.34,Part (B), No.**5**,pp. 629–637.

[29] A. Moneem S. Rahma, Maisa'a. A. A. Khodher, 2013, Proposed Method for Partial Audio Cryptography Using Haar Wavelet Transform, *IJCCCE* Vol.13, No.**2**, pp. 11–18.

[30] A. Moneem S. Rahma, Maisaa Abid Ali k., 2014, To Modify the Partial Audio Cryptography for HaarWavelet Transform by Using AES Algorithm, *Eng. & Tech. Journal* , Vol.32,Part (B), No.**1**, pp. 169–182.

[31] Maisa'a. A. A. K. Al-Dabbas, A. Alabaichi, and A. S. Abbas,2020,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, doi: 10.12928/TELKOMNIKA.v18i6.15847.

[32] Maisa'a. A. A. Khodher, Teaba W. A. Khairi,2020, Review: A comparison Steganography Between Texts and Images, *Journal of Physics: Conference Series* **1591** (2020) 012024, pp. 1–8, doi:10.1088/1742-

6596/1591/1/012024

[33] A. Malik, G. Sikka, and H. Kumar Verma, 2015, 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, doi: 10.5815/ijigsp.2015.04.08.

[34] R. T. Sabbah, 2016, A Comparable study of hiding information in images using least significant bit (LSB) substitution and pixel value difference (PVD) Method.

[35] M. Hussain, A. W. Abdul Wahab, Nor Badrul Anuar, Rosli Salleh ,Rafidah Md Noor,2015, Pixel Value Differencing Steganography Techniques: Analysis and Open Challenge, *IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, DOI: 10.1109/ICCE-TW.2015.7216859

[36] E. M. El-Alfy, A. A. Al-Sadi, 2012, Pixel-Value Differencing Steganography: Attacks and Improvements, 1CCIT 2012, pp: 757-762.

[37] D. C. Wu and W. H. Tsai, 2003, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, vol. **24**, no. 9–10. pp. 1613–1626, doi: 10.1016/S0167-8655(02)00402-6.

[38] K. Jung, 2015, 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).

[39] S. Prasad, A. K. Pal,2017, An RGB colour image steganography scheme using verlapping block-based pixel-value differencing, royal society open science, pp:1-14 http:// rsos.royalsocietypublishing.org.

[40] S. N. Khezr, N. J. Navimipour, 2015, MapReduce and Its Application in Optimization Algorithms: A Comprehensive Study, *Majlesi Journal of Multimedia Processing* Vol. **4**, No. 3, pp: 29-33

[41] A. Elsayed, O. Ismail, and M. E. El-Sharkawi, 2014, MapReduce: State-of-the-Art and Research Directions, *International Journal of Computer and Electrical Engineering*. pp. 34–39, doi: 10.7763/ijcee.2014.v6.789.

[42] J. Dean, S. Ghemawat, 2004, MapReduce: Simplied Data Processing on Large Clusters, OSDI 2004, pp: 1-13