

# Integrated System of Information hiding by Applying Three levels

Mustafa B. Mahmood<sup>1</sup>, Ban N. Dhannoon<sup>2</sup>

Research Scholar, Department of Computer, College of Science, AL-Nahrain University, Baghdad, Iraq, mbmr\_90@yahoo.com<sup>1</sup>  
 Professor, Department of Computer, College of Science, AL-Nahrain University, Baghdad, Iraq, bnt@sc.nahrainuniv.edu.iq<sup>2</sup>

**Abstract**— In the last years, the data security become more important issue for the essential and sensitive data, one of the techniques used in data security is data hiding technique, one of difficulty facing this technique is choosing the appropriate cover file, the spread of using of the WebP image format on the Internet, especially on social media and conversation programs, making it suitable for use as a cover file, because they represent emoji sticker, where they are used to express the feelings of the sender, so when sending it repeatedly do not raise doubt, which made it a point of strength in the exploitation of this feature by data security field. In this paper, an integrated system was proposed to protect secret messages by applied three levels to ensure the data security beside the 3-LSB algorithm.

**Index Terms**— Steganography, 3 Least Significant Bit (3-LSB), Central change.

## 1 INTRODUCTION

The importance of information security has emerged in recent years, due to the spread of computing system in all aspects of life. Therefore, researchers focused in this area on how to keep this information from exposure to theft or loss or change. It has become the field of information security of the most important areas that are being studied and developed, data security was defined as "Is to provide protection for any automated system that specializes in managing and storing and providing information" [Wil15]. There are properties must be provided by information security to the information managed by the system, which includes [Wit16]:

- Confidentiality: Information is available only to authorized persons.
- Integrity: Unauthorized changes to the Information is reject.
- Availability: Information must be available all the time to people authorized to access them when needed.

There are many techniques that are developed to achieve the data security, the most common techniques are cryptography and steganography [Kha14]. One of the most important of data security techniques is the steganography technique, which are not limited to being science but goes even further to be the art of embedding of secret data [Hus04]. The term of steganography that derived from two words in Greek "stegano-graphy" which means, "Perform the writing in secret form", steganography is the embed of "the secret data" which can be any form of digital data that represented in the computer system (message, image, sound and etc.) within another digital form for example (image, video and etc.) [Mic12].

The steganography system consists from two algorithms, the embedding and extraction algorithm and the other elements represent the inputs and outputs of the system as shown in Figure (1) are [Phi08]:

- Secret Data: Represents any sensitive secret.
- Cover File: Represents the carrier file that will embed the secret data inside it.
- Key: The key represents an optional element.
- Stego File: represents the cover file after the secret data has been hidden inside it.

- Embedding algorithm: It responsible for performing the process of hiding the secret data within the cover file.
- Extraction algorithm: the process of extracting the secret data from the stego file.

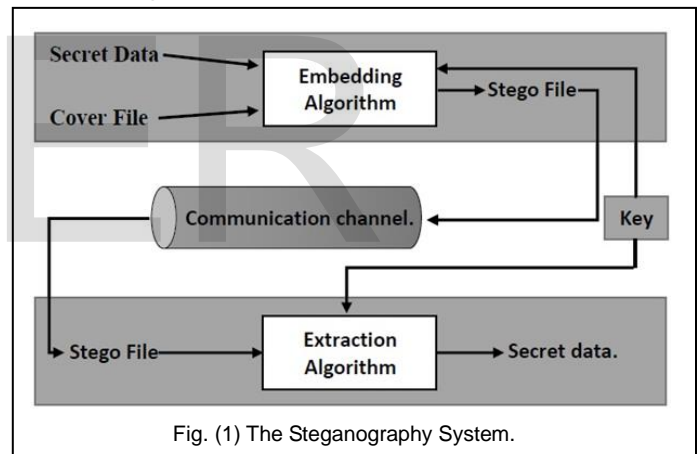


Fig. (1) The Steganography System.

## 2 THE PROPOSED TECHNIQUE

In this section, the researcher presents the proposed system by display the used algorithm and the three levels that applied on the system to achieve the aim of data security. The secret message must be convert to stream of bits. The hiding process done by hide every three bits of the secret message by using the 3-LSB. Figure (2) shows the embedding process of the 3-LSB algorithm.

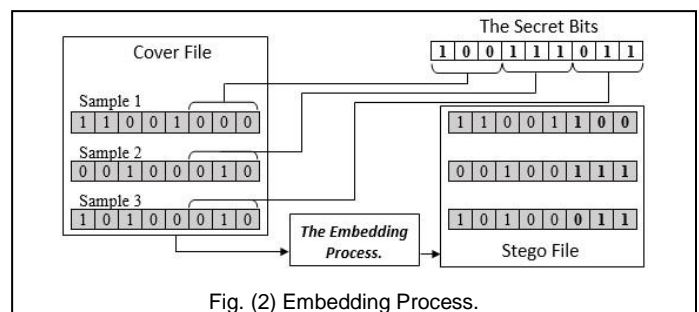


Fig. (2) Embedding Process.

**2.1 LEVEL ONE**

The first level will be applied to select the positions of the samples that data will be embed inside the value of the specific position of the cover file. The embedding process do not occur in the sequential positions, the selected positions often non-cascaded, it is begins by specify the non-transparent pixels, the output of the proposed algorithm for selection locations represent the index in the array of locations that refers to the value that represents the index in another array that represents the RGBA array that refers to the one of the three components of the pixel that use in the embedding process as a cover. Algorithm (1) shows the steps of the algorithm of selection locations to get the non-sequential index.

<b>Algorithm (1) The steps of the algorithm of selection locations.</b>
<b>Goal:</b> Generate a non-sequential index for getting value from Array of locations.
<b>Output:</b> For iteration, getting the number represent the index in array of locations.
<b>Steps:</b> From Step1 to Step5, repeated to the end of the cover file.
- Step1: initial value, let INDEX=1 and VALUE=3.
- Step2: INDEX = INDEX + VALUE.
- Step3: IF VALUE mod 3 equal 0 Then set 4 to VALUE.
- Step4: VALUE = VALUE - 3.
- Step5: VALUE = VALUE*(-1).
- Step6: IF INDEX Equal or Greater the Then cover file Then go to Step7 Else go to Step1
- Step7: End

**2.2 Level Two**

In this level, the secret message convert to an array of bits, then convert every three bits to a digit number then store it in array of digits, in this level the system was improved by redistributing the bits of the secret message, the redistribution process occurs for every digit, by reconvert every digit to the three bits then distributed these bits randomly then get the digit from the result of the process and finally; hide the randomized digit. The redistribution process require the random sorting for these three bits, for producing this random range a special function in the programming language that used to programmed the system. Figure (3) shows the example about the redistributed process. The Random function, requires two parameters to produce the final result that represents the redistributed value. The secret digit value before the redistribution process represent the first parameter, the second parameter represent the seed number, this parameter represent the key of the randomization process. Each secret digit value with a specific seed number that is sent to the random generation function, which produces redistributed value, on the other side must send the redistributed value with the same seed number to get the original value before redistribution process. In the proposed system the seed number represents the same value resulting from the proposed algorithm for selection locations in the level one that used to generate the positions of the cover values in the level one. The system use the symmetric key for steganography sharing, the seed number represent the result of the proposed algorithm for selection locations plus the symmetric key that shared between the sender and receiver.

er. Figure (4) shows the parameters of the random function with the output of the process.

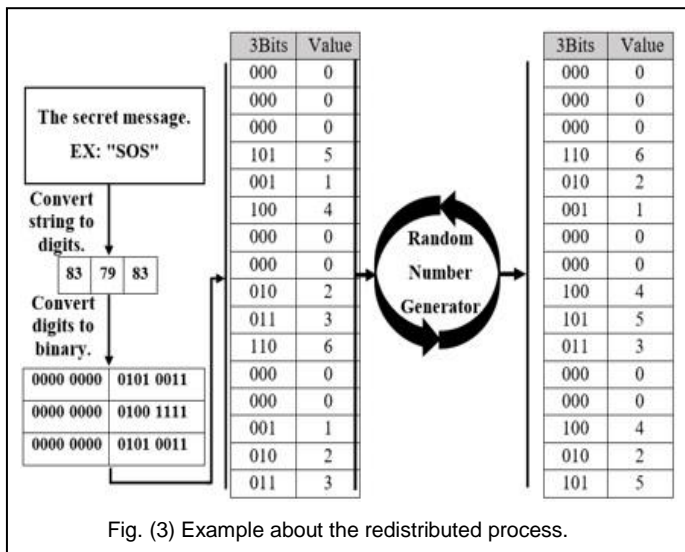


Fig. (3) Example about the redistributed process.

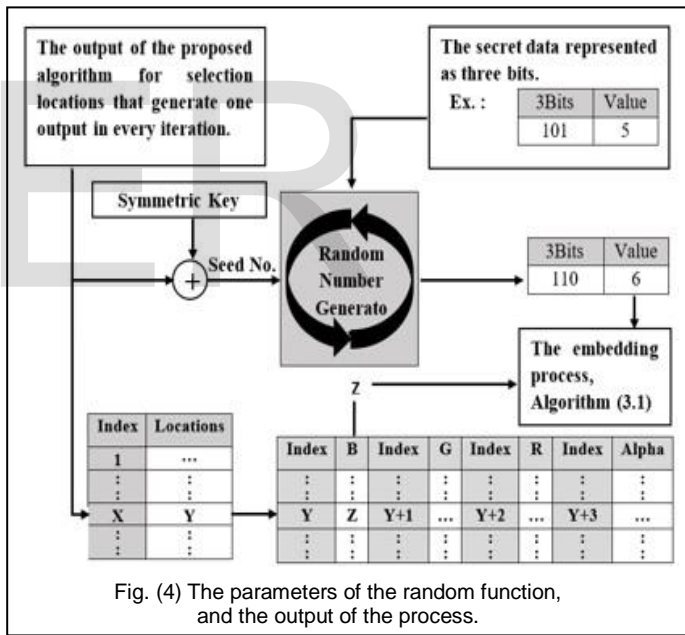


Fig. (4) The parameters of the random function, and the output of the process.

**2.3 Level Three**

In this level, one of the network security algorithms used, this algorithm is known as a RSA. The RSA algorithm used to provide two key for each user, the public key represents the first key, which it uses in the embedding process, and the private key represent the second key, only the user knows this key, so it represents the secret key. At first, the user must register in the system to generating public and private keys for each user, these keys with the name of the user will be stored, only the user name and the public key will be shared on the network. After the sender select the name from its list to send the secret message, the proposed system will be retrieved the public key for the specific name, then the system will encrypt the special

header then add it to the secret message then perform the operations of the previous two levels, Figure(5) shows the workflow of the proposed system with the three levels.

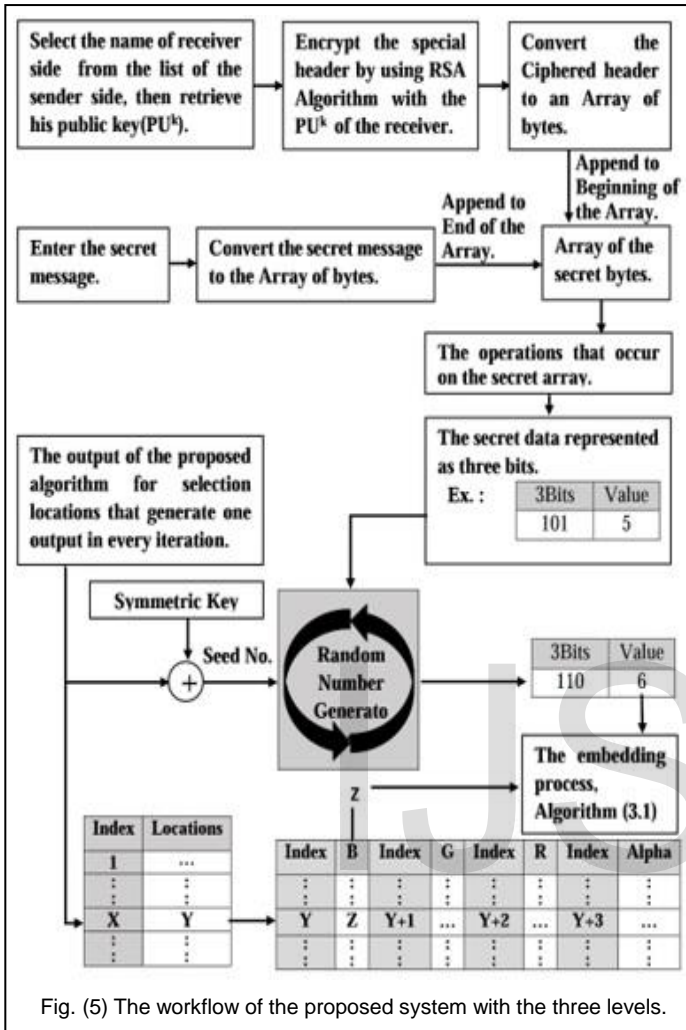


Fig. (5) The workflow of the proposed system with the three levels.

### 3 COVER FILE (WEBP) IMAGE FORMAT

The cover file, the file that carries the secret data, is different according to the algorithm used in the steganography technique, therefore, a cover file must be select that is not affected by the secret data that is embedded inside it. It also has the capability to embed as much secret data as possible [Cha13]. WebP extension can be used as a cover file, as a result of the needed to make the web browser more rapid, google has developed a new image format in the 2010, so that the size of these images format is less while maintaining image quality, this format is the WebP image format, the WebP less size from the jpeg image format by 25-34% and less size from the png image format by 28% [Tre12]. The main purpose of developed the WebP image format, is that 65% of the multimedia that consuming Internet speed is an image, so the need to develop image extension with fewer size of traditional images while maintaining image quality, Table (1) shows the difference between the WebP image format and the JPEG image format [Mil16].

TABLE (1)

THE DIFFERENCE BETWEEN THE WEBP IMAGE FORMAT AND THE JPEG IMAGE FORMAT.






Resolution (pixels)	16,383 × 16,383	65,535 × 65,535
Data Compression	lossy / lossless	lossy
Transparency	Yes	No
Bit depth	8/RGB+ 8/Alpha	8/RGB
Colors	16,777,216	16,777,216

### 4 THE PERFORMANCE OF THE PROPOSED SYSTEM

Table (2) below shows the results of the measures (MSE and PSNR) that used to evaluate the system performance of the proposed algorithm.

TABLE (2)

THE RESULTS OF THE MEASURES (MSE AND PSNR) THAT USED TO EVALUATE THE SYSTEM PERFORMANCE OF THE PROPOSED ALGORITHM.

Sticker	Message 1 250 byte	Message 2 500 byte	Message 3 750 byte	Message 4 1000 byte	Message 5 1250 byte
 25KB	MSE: N/A	MSE: 0.0019	MSE: 0.0028	MSE: 0.0036	MSE: 0.0048
	PSNR: 40.7	PSNR: 37.616	PSNR: 35.977	PSNR: 34.948	PSNR: 33.683
 49KB	MSE: N/A	MSE: 0.0018	MSE: 0.0027	MSE: 0.0035	MSE: 0.0044
	PSNR: 41.06	PSNR: 37.849	PSNR: 36.201	PSNR: 34.877	PSNR: 33.951
 73KB	MSE: N/A	MSE: 0.0016	MSE: 0.0025	MSE: 0.0033	MSE: 0.0041
	PSNR: 41.50	PSNR: 38.410	PSNR: 36.532	PSNR: 35.319	PSNR: 34.303

### 5 CONCLUSION

In this paper, the integrated system for information hiding is present, in this approach, every three bits of the secret message will be hide in one sample from the cover file, and are selected sites non-sequence from the cover and thereby ensure that no cover file confidential data deformation by applied level one. By applied level two, the redistribution process simulates encryption technique and the network security technique achieved by applied level three. The proposed method can produce stego file at various embedding rate with minimum or zero degradation. Experimental results show an improvement in the MSE and PSNR values of the proposed technique. The method satisfies the requirements such as capacity and quality of the stego file.

### References

[Cha13] Chandrakant B. "Payload Capacity Enhancement In The Field Of Steganography By Using Mobile Application Based Stego Technique." i-Manager's Journal on Software Engineering 7.4 (2013): pp. 31-36.

- [Mic12] Michael E.,Herbert J. "Principles of information security." 4th Edition, Cengage Learning (2012).
- [Mil16] Mile M., Miroslav M., et al. " Impact Of Jpeg-Webp Conversion On The Characteristics Of The Photographic Image." Tehnički vjesnik 23.2 (2016): pp. 505-509.
- [Phi08] Philip B., and Hans G. "Image steganography and steganalysis." Department Of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom (2008).
- [Tre12] Trevor B. "Check Image Processing: WebP Conversion and MICR Scan Android Application." California Polytechnic State University (2012).
- [Wil15] William, and Lawrie Brown. "Computer security." Principles and Practice (2008).
- [Wit16] Wittkop and Jeremy. "Building a Comprehensive IT security program." (2016).

IJSER