Crypto-Steganographic LSB-based System for AES-Encrypted Data

Mwaffaq Abu-Alhaija[1]
Department of Networks and Information Security
Al-Ahliyya Amman University, AAU, Amman, Jordan

***Abstract*—The purpose of this work is to increase the level of concealment of information from unauthorized access by pre-encrypting and hiding it in multimedia files such as images. A crypto-steganographic information protection algorithm with LSB-method was implemented. The algorithm hides AES pre-encrypted confidential information in the form of text or images into target containing image files. This method uses the concept of data concealing in the least significant pixel bits of the target image files. The proposed method relies on the use of Diffie-Hellman public key exchange protocol for securely exchanging the stego-key used for LSB as well as the public key used for encrypting the secret information. The algorithm ensures that the visual quality of the image remains unchanged, with no distortions perceived by the human eye. The algorithm also complicates the detection of concealed information embedded in the target image with use of PRNG as an enhancement for LSB. The proposed system scheme achieved competitive results. On an average, the system achieved a Peak Signal-to-Noise Ratio (PSNR) of 96.3 dB and a Mean Square Error (MSE) of 0.00408. The results obtained demonstrate that the proposed system offers high payload capabilities with immunity against visual degradation of resultant stego images.**

Keywords*—Steganography; cryptography; cryptographic steganography; crypto-steganographic system; Least-Significant Bit Replacement (LSB-method); stego-key; public-key cryptography; Advanced Encryption System (AES); Diffie-Hellman protocol; key exchange; concealment of information; PRNG

I. Introduction

Due to modern technology, information plays a big role in a massive number of different fields. This information varies in its nature from personal, to economic, to technological, or even governmental. When storing, transmitting, or merely using information, there is an increasing necessity to sustain its confidentiality and integrity and guard it against the unauthorized access. The greater the significance of this information is, the more protection it needs. There is no absolutely 100% reliable method to encrypt information [1]. For many years Information Hiding has captured the imagination of researchers. Digital watermarking and steganography techniques are used to address digital rights management, protect information, and conceal secrets. While cryptography uses encryption to make the message incomprehensible, steganography conceals the traces of the information ever existing. The steganography can be employed on any medium such as text, audio, video and image while cryptography is implemented only on the text file thus making steganography superior to cryptography [1]. Any information, such as text, messages, images, multimedia files, etc., can be used as a data carrier. In the general case, it is advisable to use the word "message" because the message can be plaintext, cipher text, image, spreadsheet, audio or even video data [2]. Basically, any form of data that can be represented in a bitstream can be hidden through steganography [3, 4].

This proposed system will be more secure than cryptography or steganography techniques [digital steganography] alone and also as compared to steganography and cryptography combined systems. In this paper we propose an advanced cryptographic-steganography system that combines the features of cryptography and steganography. In the cryptographic steganography system, the message will first be converted into unreadable cipher and then this cipher will be embedded into an image file. Hence this type of system will provide more security by achieving both data encoding as well as data hiding.

The purpose of this work is to increase the level of concealment of information from unauthorized access by pre-encrypting and hiding it in multimedia files such as images. This method proposes a new approach to public-key steganography based on LSB method to hide the secret pre-encrypted information inside 24-bit image file. The proposed method relies on the use of a suitable public key exchange protocol (such as Diffie-Hellman) for exchanging the stego-key used for LSB as well as the public key used for encrypting the secret information.

II. Related Work

The development of global computer networks and multimedia tools has progressed dramatically over the past few years. Consequently, new methods of data-secured transmission through telecommunication channels are continuously being developed and are used for various purposes. These methods make it possible to hide messages in computer files (containers), due to the natural inaccuracies of the sampling devices and the redundancy of analog video or audio data. Advances in technology have allowed steganography (meaning hidden writing) to occupy a certain position in the field of information encoding and its concealment. Such a trend has emerged in the field of information security as computer steganography (the secret message is hidden in other than original media such as Text, Image, video and audio form) [1-4]. The general idea of hiding some information in digital content has a wider class of applications that go beyond Steganography. The techniques involved in such applications are collectively referred to as information hiding. Methods that use image files are the most advantageous and promising, since their use is not limited by the amount of data transferred, for it all depends on the container selected. A special case of information hiding is digital watermarking. Digital watermarking is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Basically, it is advised to use the LSB approach [5] [7], which allows for a replacement that is not generally visible to the human eye; i.e. of less significance. Furthermore, many older output devices will not even be able to reflect such minor changes [8]. This approach allows replacing not only the two lower bits, but any number of bits. Although replacing more bits allows for more information to be hidden, however the greater the distortion will result in the original image [9].

Unlike information hiding and digital watermarking, the main goal of steganography is to communicate securely in a completely undetectable manner. A steganography task is to hide a certain message in another container file, so that the presence of the hidden message cannot be seen [2, 3]. As containers, digital images, audio and video files are commonly used [2, 5, 7]. As a result of embedding, steganography overcome the limitation of cryptography by hiding the fact that a transmission through the communication channel is taking place.

Both steganographic and cryptographic techniques are have proven to be powerful and robust. Alas, steganography and cryptography have been noted to be individually insufficient for complete information security. While steganography supports only Confidentiality and Authentication security principles, cryptography supports Confidentiality and Authentication security principles as well as Data integrity and Non-repudiation. Therefore, many researchers suggest a stronger and more reliable mechanism through combining both [16] [17], i.e. a crypto-steganographic system. Crypto-steganographic systems have great potential to increase information security.

III. The Basic Steganography Technique

There are special algorithms for hiding information in digital form using steganography [2, 4, 6]. Adding information to existing files (such as multimedia files) leads to distortions that are below the human sensitivity threshold, thus there is no noticeable change in the perception of the input files. The steganography technique involves a container (cover carrier), built-in secret message, and possibly stego key:

- Built-in (secret) message-a message embedded in a container.
- Container files - any file intended to conceal secret messages in. Empty containers, also known as cover files, are containers without a built-in message, whereas a filled container or stego object is a container that contains embedded information.
- A stego key or just a key is the secret key needed to control the stego process in selecting the actual image pixels to be used to conceal/extract information.

LSB (Least significant bit) replacement is the most common, yet simplest, method to embed information into container files [8]. The least significant bit the container file bytes is replaced by a bit of the secret message. LSB works best with 24-bit map images (BMP), in which each pixel is represented by 3 bytes (red, green, blue color components consecutively). Consequently, LSB allows to store 3 bits of information in one single pixel, replacing one bit of each color component. Thus, using a 256*256 image, LSB can store 196608 bits (i.e. 24576 bytes) of embedded data.

To demonstrate LSB replacement, the number 62 is to be embedded in a BMP image file. Converting 62 to binary yields 111110, requiring a grid for 2 pixels of a 24-bit image. An example grid of 2 pixels can be as follows in Table I.

Replacing 111110, the binary representation of 62, with the least significant bit of this part of the image results in the following grid of Table II.

Even though 62 was embedded into 2 bytes of the grid, only one single bit actually changed, depending on the embedded number. It has been found that on average only half the bits in a given image will need modification [7, 8, 10]. Given the fact that each primary color has 256 possible intensities, applying LSB results in small color intensity difference which is not perceived by the human eye.

In its simplest form, LSB makes use the lossless compression provided by BMP images. As shown above, consecutive bytes of the image data are used to embed the information, starting from the first image pixel for every byte of the message in successive order. Consequently, LSB in its most basic form is vulnerable and very easy to detect. As a remedy to achieve a more secure version of LSB, it is advised that the communication parties share a secret key. A stego-key refers to the secret key used to specify which pixels to target with LSB. Without prior knowledge of such a key, there would be no way of knowing which pixels actually contain embedded information. Fig. 1 below demonstrates the operation of stego-key enhanced LSB steganography.

An overview of the existing methods of solving the problem [2, 3, 5], showed that the most promising in terms of information capacity are containers in the form of image files in BMP format. Methods that use image files are the most advantageous and promising, since they practically do not limit the amount of data transferred, it all depends on the container selected. They also provide a high degree of protection. Therefore, they are better used in future implementations [7] [10]. For the steganographic algorithm proposed, it is advisable to use the LSB method and BMP image files as containers.

TABLE. I. An Example 2-Pixel Grid of a 24-Bit BMP

RED	GREEN	BLUE
00101101	11000100	01100011
00001101	00110011	10101010

TABLE. II. Adjusted Pixel Grid after Applying LSB

RED	GREEN	BLUE
0010110***1***	1100010***1***	0110001***1***
0000110***1***	0011001***1***	1010101***0***

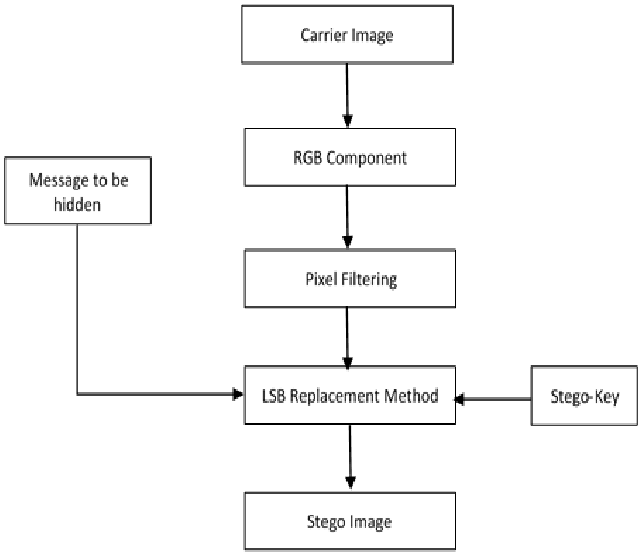


Fig. 1. Stego-Key Enhanced LSB Algorithm.

IV. Cryptographic Steganography

The basic steganography technique does not employ changes in the structure of the message in an attempt to achieve secure and undetectable communication. Nonetheless, a steganosystem could have the ability to embed a pre-encrypted message. The embedding process may depend on a secret stego-key. The stego-key is used to control the embedding process, such as the selection of pixels or coefficients carrying the message, etc. One or more stego-keys can be included in a steganosystem, depending on the number of security levels intended [12, 13, 16]. Similar to cryptographic systems, steganography can also be done using a private key (i.e. secret key steganosystem) or a public key (public key steganosystem). A secret key system uses a single key that must be defined either before the start of the secret message exchange or transmitted over a secure channel. This option is less effective because the attacker gains access to the data by intercepting the key. Public key steganosystems use different keys for embedding and retrieving messages, such that one key cannot be deduced from the calculations. Therefore, one key (public) can be freely transmitted over an unsecured communication channel. In addition, this scheme work well with mutual distrust of the sender and the recipient. Therefore, choosing such a key is more useful and provides a high level of security.

The system proposed by author adopts LSB method to replace the least significant bits in the container (image, audio, or video) with the bits of the hidden message. To increase the level of security of the proposed system the hidden message can be pre-encrypted using public-key encryption prior to embedding it into container file. The proposed system makes sure the difference between empty and filled containers is imperceptible to human senses, while maintaining the integrity of the embedded message without any data loss.

The flow chart of Fig. 2 gives the structure of the algorithm proposed by the author. The proposed method describes 2 phases for hiding the secret information by using the public steganography based on matching method in different regions of an image.

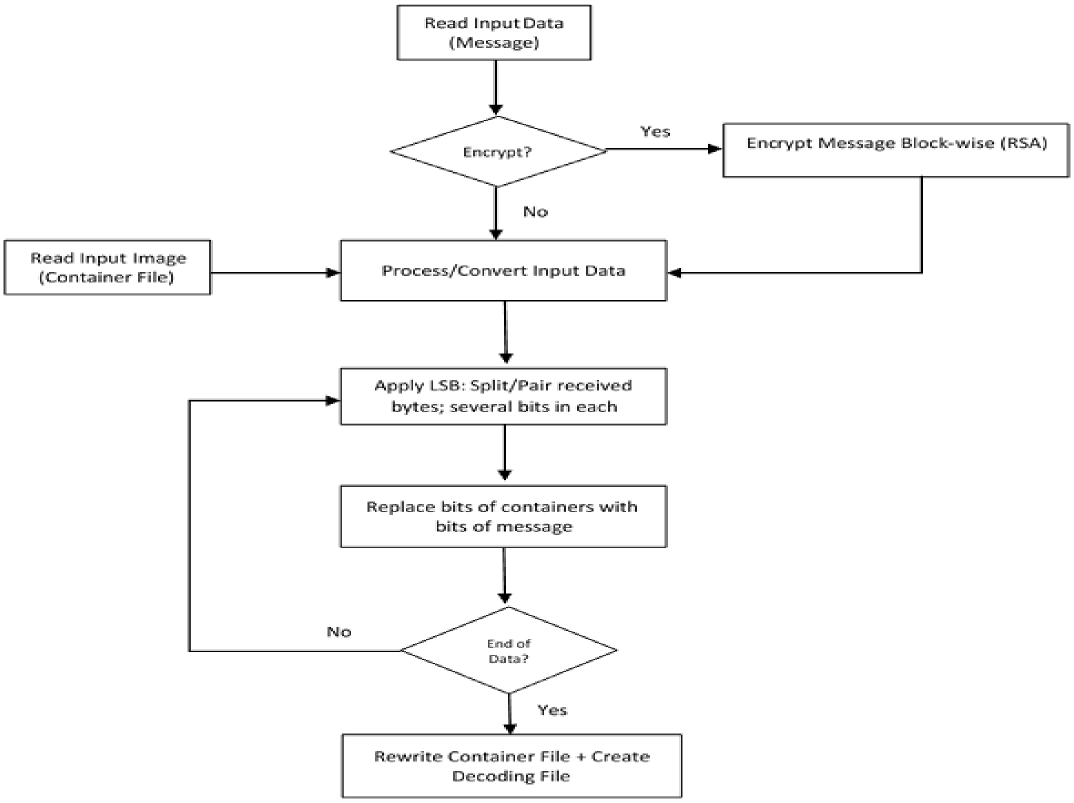
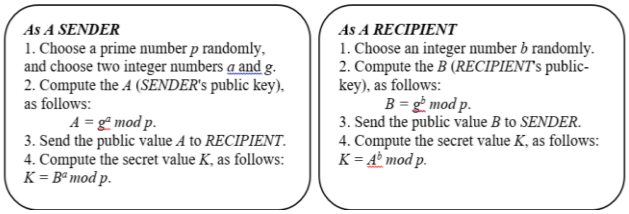

Read Input Data (Message)
Encrypt?
Yes
Encrypt Message Block-wise (RSA)
No
Read Input Image (Container File)
Process/Convert Input Data
Apply LSB: Split/Pair received bytes; several bits in each
Replace bits of containers with bits of message
No
End of Data?
Yes
Rewrite Container File + Create Decoding File

Fig. 2. Flowchart of Proposed Algorithm.



As A SENDER

1. Choose a prime number *p* randomly, and choose two integer numbers *a* and *g*.
2. Compute the *A* (*SENDER*'s public key), as follows:
   $A = g^a \; mod \; p$.
3. Send the public value *A* to *RECIPIENT*.
4. Compute the secret value *K*, as follows: $K = B^a \; mod \; p$.

As A RECIPIENT

1. Choose an integer number *b* randomly.
2. Compute the *B* (*RECIPIENT*'s public-key), as follows:
   $B = g^b \; mod \; p$.
3. Send the public value *B* to *SENDER*.
4. Compute the secret value *K*, as follows: $K = A^b \; mod \; p$.

Fig. 3. Diffie-Hellman Key Exchange Protocol.

The first phase involves converting the Plain text message into cipher text using Public-key Encryption algorithm. The proposed algorithm performs AES block-wise encryption [18]. The two communication parties (SENDER & RECIPIENT) exchange the public keys over insecure networks by applying Diffie-Hellman Key exchange protocol [19]. Public key exchange cryptosystem like the Diffie-Hellman Key exchange protocol eliminates the key distribution problem by using two keys, a private and a public key. By exchanging the public keys, both parties can calculate a unique shared key, known only to both of them. Fig. 3 depicts the steps necessary for a successful Diffie-Hellman Key Exchange.

The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array [18]. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. For the purpose of the proposed method, 10 rounds of transformation was adopted resulting in a 128-bit key.

The AES encryption cipher first undergoes a substitution of data using a substitution table; followed by shifting the data rows, then mixing of the columns, finally reaching the last transformation with a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key. As AES is considered a symmetric data encryption technique, the same secret key can be used for both encrypting and decrypting.

The next phase is to find the shared stego-key between to be used for enhancing LSB. The authors in [10] and [11] studied the use of a Pseudo Random Number Generator (PRNG). Pseudorandom number generator acts as a black box, which takes one number (called the seed), and produces a sequence of numbers. The output generated is a random bit position from 7 most significant bits for each R, G and B values of each pixel of the image. Each of these bits will undergo an exclusively-OR operation with one bit of the message in successive order, then embedding the result in the least significant bit. The parameter controlling PRNG (i.e. the seed) ensures generating the same sequence of number in the same sequence. The author of this work proposed encrypting the PRNG parameter using AES with the key generated by applying the Diffie-Hellman Key exchange protocol, to finally send it over to recipient.

The detail of the second phase of the proposed algorithm is shown below in Fig. 4. The resultant stego image can be sent over unsecured communication channels to the intended recipient.

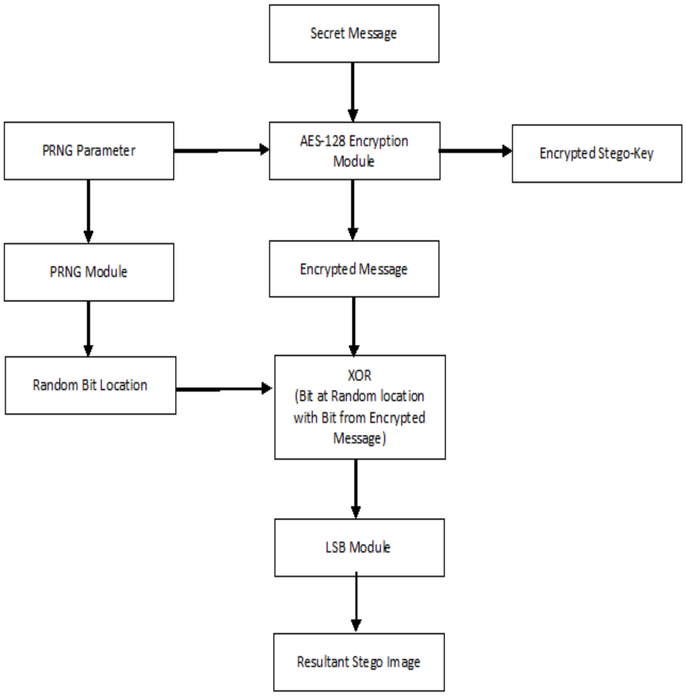


Fig. 4. Details of Proposed Algorithm.

V. Experimental Results

The proposed algorithm has been implemented, in separate modules for LSB, PRNG, Diffie-Hellman, and AES public key encryption. The performance of the proposed implementation has been tested through the use of different secret messages in varying lengths. Each message used was hidden in different 24-bit RGB cover images. The same experiments were performed for 512x512 and 256x256 standard images to properly evaluate the effectiveness of the proposed method.

The two major metrics for evaluating picture quality are Mean Square Error (MSE) [14] [16], and Peak Signal to Noise Ratio (PSNR) [15] [17].

MSE is the measurement of the square of error, the error is the amount by which the original image's pixel value is different to the encrypted image's pixel value. MSE can be calculated as follows [14] [16]:

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{[f(i,j) - f'(i,j)]^2}{MN} \qquad (1)$$

M and N represent the image’s height and width respectively. The term $f(i,j)$ is the pixel value at row i, column j of the original image and the term $f'(i,j)$ is the value of the pixel at the same location of the decrypted image.

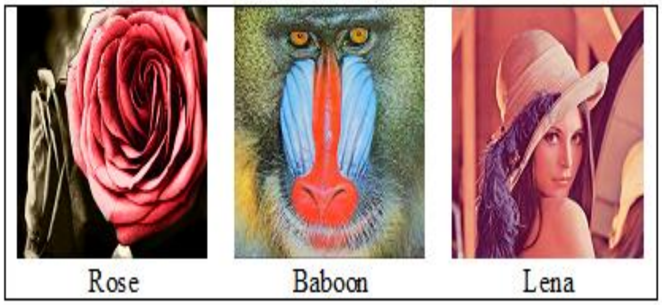
PSNR represents the ratio between the maximum probable signal power and the power of corrupting noise which influences the fidelity of its representation. PSNR is typically represented in terms of the logarithmic decibel as follows [15] [17]:

$$PSNR = 10 * \log \frac{(2^n - 1)^2}{MSE} \qquad (2)$$

The implemented method has been evaluated using MATLAB using three popular images (Rose, Lena, and Baboon), in both sizes 512x512 and 256x256, as shown in Fig. 5. Message lengths for 512x512 image experiments ranged from 16KB to 64KB. On the other hand, for 256x256 image tests, message lengths ranged between 4KB and 16KB.

As a sample visual image comparison, the Rose image is shown before and after the application of the proposed method. For better visualization, both images are shown side-by side in Fig. 6. It is clear that the resulting distortion can be barely perceived by the human eye. Nonetheless, this visual outcome was further tested mathematically through calculating the PSNR and MSE values.

A high PSNR reading indicates a high quality of a stego image. Researchers consider a PSNR reading of above 40db for stego images to be considered as good quality images [18]. The MSE and PSNR results are shown in Table I and Table II, for the 512x512 and 256x256 experiments respectively. It has been proven that the resultant stego images; the Rose image as an example, had very high PSNR values.



(a) (b)

Fig. 5. Cover Images Used for Evaluation.

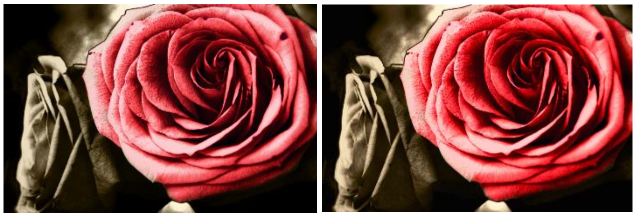


Fig. 6. Sample Image Comparison: (a) Rose Original Image, (b) Rose Modified by Proposed Method.

TABLE. III. MSE AND PSNR VALUES FOR 512X512 COVER IMAGES

Cover Image (512x512)	Message Length	MSE	PSNR
Rose	16K	0.00195	99.29586
	32K	0.00227	98.63595
	64K	0.00352	96.73078
Baboon	16K	0.00219	98.79176
	32K	0.00236	98.46709
	64K	0.00298	97.45404
Lena	16K	0.00332	96.98482
	32K	0.00457	95.59704
	64K	0.00504	95.1719

TABLE. IV. MSE AND PSNR VALUES FOR 256X256 COVER IMAGES

Cover Image (256x256)	Message Length	MSE	PSNR
Rose	4K	0.00432	95.84137
	8K	0.00469	95.48448
	16K	0.00501	95.19783
Baboon	4K	0.00436	95.80134
	8K	0.00469	95.48448
	16K	0.00482	95.36574
Lena	4K	0.00549	94.80048
	8K	0.00575	94.59953
	16K	0.00611	94.33579

The proposed system scheme achieved competitive results. On an average, the system achieved a Peak Signal-to-Noise Ratio (PSNR) of 96.3 dB and a Mean Square Error (MSE) of 0.00408. The results obtained demonstrate that the proposed system offers high payload capabilities with immunity against visual degradation of resultant stego images. In comparison with standard LSB, the proposed system obtained the same PSNR values, except for the fact the secret message is actually hidden in a random bit position. Due to this random position situation, even if attackers are certain of its existence, they cannot retrieve the secret message without prior knowledge of the system's stego key for PRNG. The added security provided by AES encryption, diminishes the chance of successful attacks. Hence, the proposed method has proven to provide robust, secure image steganography for secured communication.

VI. CONCLUSIONS

The algorithm of steganographic protection of information according to the LSB method is developed, and the program code is implemented, which increases the level of protection of information from unauthorized access by hiding it in multimedia files, namely in image files. Hiding data occurs in the lower bits of the pixels of the image files while randomly selected bit locations of the pixels manipulates the standard LSB replacement policy, thus concealing the reference of the real data. The algorithm does not change the visual quality of the image, which makes it impossible to detect the fact of hiding information. Testing completely confirmed the correctness of the algorithm and the software. The results obtained demonstrate unnoticeable image degradation making it almost impossible to attract the attention of attackers.

This method will provide more security to the information being transmitted than any other cryptographic or steganographic system as it combines both features. On one hand, extra level of security can be achieved by using grid cipher encryption. On the other hand, distortion in the final multimedia image will be very negligible as we are using modified bit insertion technique. The proposed system is believed to be applicable to various areas such as: Confidential communication and secret data storing, Protection of data alteration, Access control system for digital content distribution, as well Media Database systems with the help of advanced sorting algorithms [20].

Future work aims at attempting to try applying the proposed algorithm and implemented system on audio and video messages, in hopes of obtaining competitive results. On the other hand, further studies will aim at enhancing (i.e. increasing) the proposed system's capacity to much larger message lengths while maintaining similar PSNR readings. The author intends to further study the possibilities of broadening the areas to which this proposal can be applied.

References

[1] Taha M S, et al. "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019), IOP Conf. Series: Materials Science and Engineering, 518 (2019), doi:10.1088/1757-899X/518/5/05200.

[2] Douglas M, Bailey K, Leeney M and Curran K, "An overview of steganography techniques applied to the protection of biometric data", Multimedia Tools and Applications, July 2018, Volume 77, Issue 13, pp 17333–17373.

[3] AL-Shaaby A and AlKharobi T, "Cryptography and Steganography: New Approach", Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 25-38.

[4] Arya A and Soni S, "A Literature Review on Various Recent Steganography Techniques", International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-4248 Volume: 4 Issue: 1, January 2018 pp: 143 – 149.

[5] KASAPBAS M and ELMASRY W, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sådhanå, (2018), 43:68 Indian Academy of Sciences, https://doi.org/10.1007/s12046-018-0848-4.

[6] Pradhan A, Sekhar, and Swain G, "Digital Image Steganography Using LSB Substitution, PVD, and EMD", Hindawi Mathematical Problems in Engineering, Volume 2018, Article ID 1804953, https://doi.org/10.1155/2018/1804953.

[7] Pelosi M, Poudel N, Lamichhane P, and Soomro D, "Steganography System with Application to Crypto-Currency Cold Storage and Secure Transfer", Advances in Science, Technology and Engineering Systems Journal, Vol. 3, No. 2, 271-282 (2018), ISSN: 2415-6698.

[8] Akinola S. and Olatidoye A., "On The Image Quality And Encoding Times Of LSB, MSB And Combined LSB-MSB Steganography Algorithms Using Digital Images", International Journal of Computer Science & Information Technology (IJCSIT), Vol 7, No 4, August 2015.

[9] Zakaria A, et al. "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution", Applied Sciences. 2018, 8, 2199; doi:10.3390/app8112199, www.mdpi .com/journal/applsci.

[10] Ali, Sohrawordi, Uddin, "A Robust and Secured Image Steganography using LSB and Random Bit Substitution", American Journal of Engineering Research (AJER), 2019, E-ISSN: 2320-0847, p-ISSN: 2320-0936, Volume-8, Issue-2, pp-39-44.

[11] Emam, Aly, Omara, "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 3, 2016 page 360.

[12] Swain G, "Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution", Arabian Journal for Science and Engineering (2019) 44: 2995–3004, https://doi.org/10.1007/s13369-018-3372-2.

[13] Ramakrishna M et al, "Securing Information: Cryptography and Steganography", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, pp 4251 – 4255.

[14] Jaryal S. and Marwaha C., "Comparative Analysis of Various İmage Encryption Techniques", International Journal of Computational Intelligence Research, ISSN 0973-1873 Volume 13, Number 2 (2017), pp. 273-284, Research India Publications, http://www.ripublication.com.

[15] Zena M. Saadi and Matheel E., "Image Encryption Using DNA Addition", Thesis, Computer Science Department, University of Technology, 2017.

[16] Rahmani K, et al., "A Crypto-Steganography: A Survey", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014, pp 149-155, www.ijacsa.thesai.org.

[17] Aung P P and Naing T M, "A novel secure combination technique of steganography and cryptography", International Journal of Information Technology, Modeling and Computing (IJITMC), 2014, 2, pp: 55-62.

[18] Kaur G and Madaan N, "A Comparative Study of AES Encryption Decryption", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064 Volume 3 Issue 4, April 2014.

[19] Whitfield Diffie and Martin Hellman, "New directions in cryptography", Institute of Electrical and Electronics Engineers., vol. IT-22, Transactions on Information Theory, no. 6, 1976, pp. 644–654.

[20] M. A. A. Alhija, A. Zabian, S. Qawasmeh, and O. H. A. Alhaija, "A heapify based parallel sorting algorithm," Journal of Computer Science, vol. 4, no. 11, pp. 897–902, 2008.