FSK Modulation Based Image Steganography

FSK Modulation Based Image Steganography

Ahmad Habboush
Department of Computer Science
Faculty of computer Science and Information Technology
Jerash Private University
ahmad_ram2001@yahoo.com

Abstract

Steganography is a method of hiding information inside a cover. Several algorithms were developed to hide secret messages inside digital media such as image, audio, video and text. Prior researches focused their efforts into two main issues: the security of the secret message before embedding and complexity of intelligent work to achieve a reliable message hiding inside the cover. This paper introduces a new steganography technique that addresses the security issue based on multi-level security by applied wavelet transformation and digital modulation. The secret message is being modulated inside the cover by using wavelet domain. This method will add high security to the secret message with robustness to external attackers. The experimental results have shown that the peak signal-to-noise ratio (PSNR) is near 50 db without detecting the secret message after embedded in the cover.

Keywords*: Steganography, Modulation, Wavelet Transformation, Message Security*

1. Introduction

Secrecy of information is being considered as a high priority issue since ancient time. The information that contains messages has two security weaknesses; storing the secret message, and message transformation. From ancient time, human faced a big challenge to hide transferred message from source to destination. Initially, focal messages were very powerful, but it has many limitations and it costs much higher. In fact, not all focal messages are possible to be transmitted. Transmission depends on many factors, including finding the message holder people which is considered to be a very danger issue and needs special treatment. Also, the transfer of human is costing much more than the transferring of written message which is possible to be attached with many different methodologies [1].

The security of the message was raised from the importance and secrecy of the data that included in the message. So, early human methodologies was very simple and based on hiding the message either by the use of vocal messages or by putting the paper that the messages was written on in a very secure location [2]. As human knowledge improved, active methodologies was implemented to hide the message itself, not only the paper that contains the message. In ancient Islamic world the interested politicians was innovated the etching messages which is based on writing the message as a tattoo on a shaved messenger's head and keep the messenger secret until his hair grows on and hide the message [3].

In modern centuries, a common practice have been used for very long time with some efficiency is to hide the information using chemical reactors of ink materials. It was known as invisible inks. The invisible inks cold be extracted from milk, vinegar, and fruit juices. This technique was invented by German intelligence.

Nowadays, modern technology increases the problem of data security and enlarges the problem of hiding the data using old methodologies. In fact, the paper messages become rare in the age of cellular communications and internet technology. Inaddition, modern detection and inspection methodologies become highly capable of detecting any text written in special ink or special methodologies on papers; such as infrared or x-ray inspection. This triggers the modern computer artificial intelligence to start researches in intelligent computations to hide the message in effective and efficient way.

The secret messages since ancient time until now are categorized into two fields; cryptography and steganography [4]. The steganography is the art of hidden the message, while the cryptography comprises that the message is shown but its content is not understood. In computer digital world, the cryptography was adapted by the means of encryption/decryption of information while transfer and storage. In contrast, the steganography is to hide the message itself, where the hacker do not know if there is a message or not. Hiding the message itself eliminates the trials to break the message secrecy. In modern years, the computer technology added more complexity and flexibility in data communication. The messages become very easy to be transported. The cryptography were adapted and improved in terms of data encryption and compression, whereas the steganography becomes more common in image, sound and video files. The line inspector do not know if the multimedia file has additional hidden message [3].

Hiding information in digital media is concerned in protecting data from attack while transfer over internet or any other digital media, but also, it may concerns in protection while storage media.

(i.e. CD, HDD, DVD, USB-stick ... etc.). Steganography is commonly known as intelligent data transfer security. It is represents adaptive and cheap way for transfer. Moreover, for secret communications no direct transfer channel is being used, the sender can upload a photo to the internet and the receiver can download it safely. Actually, the user is intended to upload any photo for any purpose to his internet browser, for example, uploading personal pictures to social sites like Facebook, or professional sites like LinkedIn [5].

There are three main types of data hiding based on the method that is subjected to be used in retrieval of the message data. Steganography categories also fall in those three types even though the message itself is hidden. Those three types are, pure, secret keying, and public keying as shown in Figure (1).

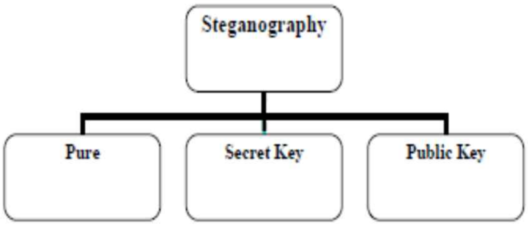


Figure 1. Steganography types [5]

The system is considered to be a pure steganography system if it does not require prior exchange of some secret information which is commonly known as key. This is the simplest way in the terms of message data retrieval. Because of that, it doesn't need any extra knowledge or any extra processing of the steganography technique that is used to hide the data. Instead, a simple process is used to extract the data directly from the stego-carrier.

Even though, this is the simplest methodology in steganography or cryptography, but it is very weak. Hence the hacker has a complete ability to break out the hidden or encrypted message. So, the need of the other two categories taken place.

In secret key steganography system, the sender selects a cover to be used to embeds the secret message inside it using a secret key. The key represents a specific data that enables reassembling hidden message from specific structure of the stego-data or crypto-data based on a predefined structure and architecture with the key terms.

The receiver extract the message by knowing the key and applied the inverse of the embedding process. Without the secret key, it could be impossible to decode the message and extract the embedded data. Secret key steganography provides much higher security than the pure one, because of the secret key. If the hacker has no knowledge about the secret key, hacking the data and extract the message from the carrier signal would not be easy.

In the public key steganography, private and public keys are used. The private key have the same specifications of the category that described in previously. While the public key is a joint that is being used to access the data with cooperation of both keys. This methodology have more complexities. Because of that, the receiver has to have a knowledge about the structure of the public key and the methodology is used to connect the two keys together. In addition, the receiver should know the private key structure. So, when the two keys are gotten by the receiver, the structure of data formulation based on corporation of those two key is needed to be gotten based on complex data analysis. This methodology increases the complexity of the system, but it adds more security level to the data security and privacy [5].

This paper presents and implements a reliable steganography-based algorithm. The goal of this paper is to implement a two level modulation based on the security of message hiding within an image that could be transferred over internet or any digital media. The results show high similarity between the original image and the stego-image. Also, the difference between the carrier and stego-image is always less than 0.1% of the image histogram difference.

The rest of the paper is organized as follows: Section 2 introduces the problem statement and formulation. Section 3 covers related work. Section 4 presents the methodology. Section 5 shows and discusses the experimentation results. Section 6 concludes the work.

2. Problem and Formulation

The steganography was first developed in the ancient time, but it suffers from limited resources and high cost which make the use of steganography not common in most cases. The politicians and postal specialists had been tried to work more with cryptography. Hence modern world becomes based on digital system and digital multimedia, the implementation of steganography based systems become more available. As a result, the use of steganography based systems is more costly efficient and uses the daily-used resources. One reason that limits the use of steganography techniques in real critical and risk applications is the hard algorithm development that needed to invent and build a real secure algorithm.

Most researchers were focusing on developing different techniques in order to implement and met the requirements that could handle the transfer of secret message. In addition, a criteria that includes security level and immunity against noise should be achieved. The big deal in steganography is that most techniques was developed to overcome low security due to direct insertion of message in the stego image. In addition, the image immunity due to distortion that caused by internet transfer, storage media and others can represent very big problem. Because of that, the insertion of the message inside the image is considered to be very weak and has no rigid structure versus low noise or even white noise. In those cases, a small amount of systematic noise can lead to lose the transferred message. Many techniques were used practically for a short time, but failed quickly because the criteria could not be achieved. The real reliable steganography technique should co-operate very high security level and immune to noise.

The highly adaptive and efficient technique that is presented in this paper has to achieve two level of security on steganography; cooperative digital frequency shift keying (FSK) modulation technique and complex mathematical formulation of wavelet transformation domain to address the described problem.

The researches that achieved applicable results are suffering many problems. The problems falls either into systematic problems due to noise, compression, or geometric processing of the image, or either into security issues due to the ease of break. The transmitted messages could have high immunity due to scale, compression, and noise if the techniques that used to hide the information inside the image depend on low noise variant [6]. This could be achieved by mathematical based solutions.

The political associations and the organizations that deals with critical data transmission are continuously motivate the researchers and push on to continue the development of steganography rather than cryptography due to its higher benefits. The wavelet transformation adds a complex mathematical domain against the attackers, in addition to stable space for modulation of data.

3. Related Work

The development of a highly secure algorithm is needed to transfer secret data over the internet by enhancing the protectiveness of the steganography. The message should be hidden in the image; this is the main headline of the research methodology. So, attacking or hacking the image contents will be very difficult, due to the variance of the coding and modulation technique that is based on multi-level security contributed approach.

The images are used as a cover objects in the steganography. That is the digital images are transferred through many communication medias such as emails. Many algorithms and methods are proposed to utilize the concept of steganography.

S.K. Bandyopadhyay et al. (2005) introduced the most common technique in Steganography, least significant bit (LSB) insertion. The approach embeds information in a carrier data. For images as a covering media, the LSB of a pixel is replaced with an M's bit. When working with 24-bit images as carrier, 3-bits can be stored in each pixel by modifying the LSBs of R, G and B array. The resulting image looks identical to the original image [7].

M.S. Sutaone, and M.V. Khandare, 2008, implement a modified steganography application. The system of steganography is being developed in order to encoding/decoding an information data file by embedding it to a target carrier image. This research uses random LSB insertion algorithm. It depends on spreading out the message data file among the carrier (cover) image in semi-random manner. Pseudorandom numbers is being generated by a key, which should identify the order of the hidden data and the data hiding algorithm [8].

N. EL-Emam, 2007, proposed an algorithm to have more level of security on LSB insertion Steganography approach. The proposed modification improves the level of security. This makes the original LSB insertion more difficult to break or attack. But it becomes weaker these days during the diffusion and common use of LSB insertion method [9].

S.K.Bandyopadhyay et al, 2009, proposed a heuristic approach of steganography in order to enable hiding huge amount of LSB data in an image. This approach firstly decodes the message data. Then during the retrieval of the encoded data, which being hidden behind a carrier image, it modifies the least significant bits of each pixel in the carrier image. The problem of this technique is the distortion of resulted image with comparison of the original one [10].

A. Emam and M.M. Ouf (2012) compared eight multi-precision libraries using a number of criteria such as performance, support of public key primitive operations, ease of use and portability. They ranked the libraries based on the performed measurement and considering the performance and relative use of primitive cryptographic operations. This study aims to measure the suitability of the libraries for wide range Public Key Cryptosystems such as RSA, DSA and Elliptic Curve Schemes. The study provides a practical recommendation regarding the optimum choice of the multi-precision library. This was based on the performance including time and resources devoted to the implementation [11].

L. Davidson et al. (2005) developed a framework for hidden message location based on image restoration. They defined two energy functions for both gray and color scale images in order t measure the energy of each pixel. The most energized pixels those with outliers. The study concludes that the stego-images contain are more energy than their cover counterparts. Moreover, the result might be improved by decomposing the image into similar regions using spatial clustering techniques [12].

R. Ibraheem and T. Kuan (2011) proposed a new steganography method based on the spatial domain instead of using LSB-1 of the cover for embedding the message. LSB-3 was used to increase the robustness. To minimize the difference between the cover and the stego-cover, it was modified according to the bit of the message. The stego-Key is used to permute the message bet before embedding the message in order to increase the message protection [13].

Anjali et al, 2011, presented a biometric based approach (skin tone) using DWT. Embedding the data in the skin area is done by encoding, and retrieve it by skin detection, the data is hidden in high frequency band of DWT. It provides PSNR and effective usable part of the image as measurements, which shows the problems of this methodology. Those problems includes low PSNR, high distortion, limited size because it uses object based hiding of the data, in addition to limitation of use on human fully skinned images [14].

J. Mandal and M. Sengupta, 2010, present a method for embedding a message in the components of DWT by direct insertion. They decomposed the image into wavelet components (horizontal, vertical, and diagonal) and directly insert the message bits in those components. The insertion was done as two bits in each byte via hash function. It provides MSE, PSNR, and standard deviation measurements that shows the problems of that paper. Those problems includes the specialization of that methodology for PPM images only, low security because it use direct insertion even though it used hash function for insertion, and high PSNR [15].

A. Al-Taby and F. Al-Naima, 2010, show an accumulative steganography of message in DWT directly by bit insertion. This algorithm is specialized for JPEG images only and comprises high PSNR, high MSE with low message size. This comes from the fact that each byte needs 9 pixels to hide it [16].

E. Ghasemi et al, 2011, present unique genetic algorithm based DWT domain steganography. The genetic algorithm is used to map and select better embed location of data inside the DWT. To select the optimal location of embedding the message byte, the genetic algorithm is being adopted. The block of optimization is 4X4 (16pixel), thus, the embedding is done via direct insertion in wavelet domain. The authors claim this methodology provide high capacity, but in fact, each byte of message needs 16 pixels to be hidden in. The histogram changes is clear between the cover images and output one. It also show a medium PSNR. [17]

P. Chen and H. Lin, 2006, introduce a methodology for data in high frequency band of DWT steganography. It uses hash table for message encoding. The stego embedding is done directly inside the wavelet domain in high frequency band, where it is a LSB insertion. This methodology is accumulative and comprises a high PSNR in addition to weak security because of direct insertion bits [18].

4. Methodology

The proposed methodology consists of two phases, in the first phase it hides the secret message (text) into a carrier image. While the second phase it retrieves the message data text from the stego-image. Figure 2 shows the general methodology of hiding the text data. On the other hand, figure 3 illustrates the methodology of retrieving text data from the stego-image.

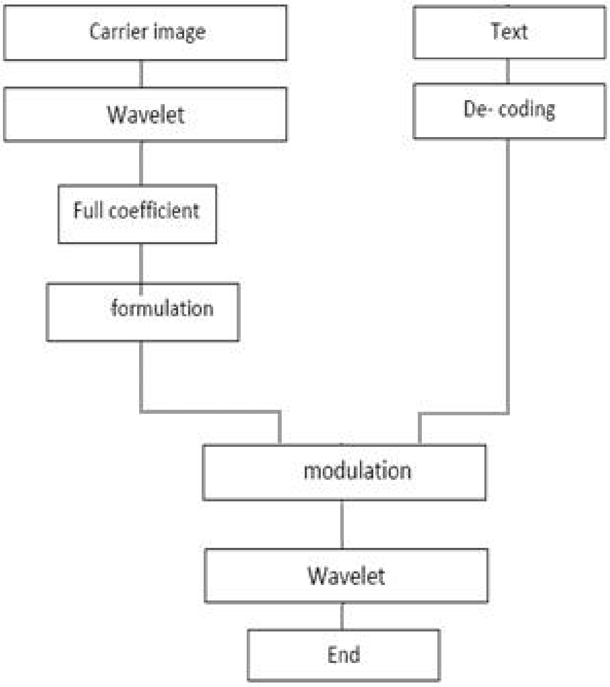


Figure 2. Block diagram of the proposed steganography technique

Initially, the carrier image and the text message file should be determined. The text message has only two constraints; the message size and the coding of the text data. This system is designed for English language; this language is represented in ASCII using 7-bit uni-code characters. Moreover, the algorithm also has the ability to deal with all keyboard special characters including "shift" operator. The special characters have ASCII coding needs more space than the formal English language context. The maximum number of bits needed to store the uni-code of the keyboard special characters is 16 bit. This enables to embed languages other than English in the stego file. The size of the text message depends only on the size of the image.

The carrier image that we need to embed the text in could be of any compression type (i.e. bmp, png, tiff, jpg, etc.). This image should be stored in either gray or event RGB colored image.

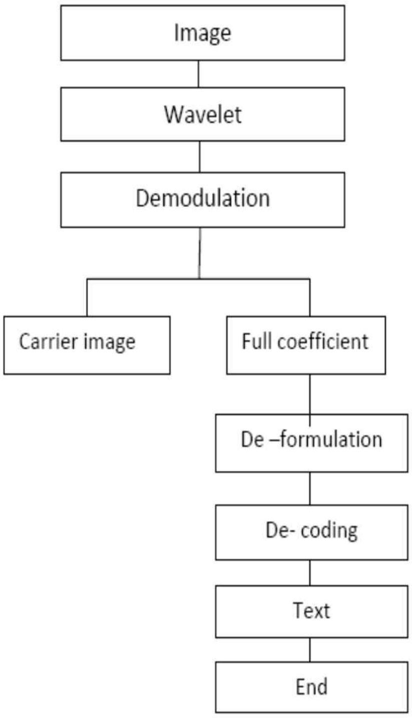


Figure 3. Text extraction from a stego-image

Starting of data collection, the carrier image can be selected by the user randomly. The message text will be transformed and expressed in a numeric matrix form. The size of input data and image capability will be calculated.

The image is by default converted to a matrix in spatial domain when reading it and retrieves the mathematical matrix that represents the image. The first security step deals with the image in complex frequency domain by the means of wavelet transformation. This domain is selected to be wavelet domain because wavelet has rich frequency parameters and doesn't have simple periodic like Fourier transform. The wavelet parameters are harder to be predicted and not capable to be simply fetched by statistical analysis.

In order to limit the size of the message that is embedding inside the image, a signature is being used. The actual problem is that, the message resolution could be very large. For example, a normal PDA camera is now commonly to be 5 mega pixel and more, while a common digital cameras are around 15 mega pixels. This large size of the image consumes a lot of processing power. If the message size is small with respect to carrier image size, then there is no need to make processing for the overall image in the receiver terminal. To avoid that, a signature is being added to the message after converting it to a crypto data.

The signature is being added by the transmitting terminal, while the receiver is intended to keep search inside the image to extract the message contents after getting the signature. The modulation of the crypto message inside the stego-image is being done via wavelet transformation. The image first transformed to wavelet, and then the modulation is done with respect to wavelet. Finally, it converted again to the image domain.

Hence, wavelet transformation is a hybrid time-frequency transformation, so, the security is by default very high. Because of that, the statistical and accumulative detection programs is capable to work with image pixels directly. Furthermore, these programs capable to work with frequency domain by treating the image using Fourier transformation. But when working with wavelet transform, the statistics become useless to detect any inconsistency in the image data.

The process of feature extraction is to extract a set of essential characteristics that can identify or represent whole of specific signal. Hence the image is being represented as a two dimensional signal which contains many unique characteristics that are specific for each individual, and information that allow to make complex mathematical operations on it.

Different methods could be used to process an image: Discrete Fourier Transforms (DFTs), Discrete Cosine Transform (DCT), Wavelet Transform etc. Wavelet Transform provides a useful decomposition of a signal, so that faint temporal structure can be revealed and handled by nonparametric models. Using wavelets allows analyzing the signal at several levels of resolution, which make it possible to capture transient, high-frequency bursts with poor frequency resolution and slowly varying characteristics with high-frequency resolution. This make it possible to trade-off frequency resolution for better time resolution (for analyzing transients) and time resolution for better frequency resolution (for analyzing slow variations).

This research is concerned with using wavelet transformation as a med step for modulating data inside a two dimensional digital signal (image) Transform of a signal. It does not change the information content, however, it presents it in the signal.

The modulation has a typical role in analog and digital communication system. The basic modulation criteria are common in different modulation methodologies. Those criteria determine the modulation scheme and selectivity. The modulation could be performed on analog message signal, thus it is called analog modulation or could be performed on digital message signal, and thus it is called digital modulation.

Three types of digital modulation are reliable and commonly used in different communication systems; those are Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), and Phase Shift Keying (PSK). Frequency Shift Keying (FSK) is the earliest digital modulation technique that used in the communication commercial technology. It could be performed on either discrete (multi-valued) message signals or on digital (binary) message signals. In the first case it called Discrete FSK while on the second it is called Binary FSK.

The basic concept of the FSK is very simple. First, let’s consider the Binary FSK, the signals transmitted for marks (binary ones) and spaces (binary zeros) are mathematically expressed as equations (1) and (2) respectively.

$$s_1(t) = A \cos\ (\omega_1 t + \ \theta_c), \qquad 0 < t\ \leq T \qquad (1)$$

$$s_2(t) = A \cos\ (\omega_2 t + \ \theta_c), \qquad 0 < t\ \leq T \qquad (2)$$

Where A is the original value of the sample. ω1, ω2 are frequencies of modulation those are being gotten from wavelet transformation. t is the sample time step. s1 is the mark modulation result. s2 is the space modulation result. Ɵ1, Ɵ2 are the modulation values.

In this paper, mark and space modulation are being used to modulate logical 0 and 1. If the encoded bit of the text message is 0 then, the space is modulated within the image, while if the encoded bit of the text message is 1, then, the mark is modulated within the image.

The resulted image is capable to be transmitted using any of the digital media hardware like mass storage, hard drives, compact drives, etc. or could be transferred via internet using email, web pages, or even social media. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and the compressed image. The higher the PSNR is the better the quality of the compressed or reconstructed image.

MSE and PSNR are two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower value of MSE is the lower the error. To compute the PSNR, the block first calculates the mean-squared error using the following equation (3).

$$M\,SE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (3)$$

Where, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation (4).

$$PNSR\ = 10\log_{10}\left(\frac{R^2}{M\,SE}\right) \qquad (4)$$

Where, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc.

Capacity represents maximum size of the text that can be loaded into image. In order to compare capacities used by different methods, the text size should by calculated as a percentage of the full capacity by using equation (5).

$$\frac{Characters\quad count}{image\quad size} * \ 100\% \qquad (5)$$

For example if we use an image with size equal to 50x50 and the maximum number of characters that can be loaded in this image =1599 characters, then the maximum size or (capacity) of this image equals (1599\50x50)*100=63.96%.

5. Results

Initially, the results are being estimated on the same computer. But to make the process more practical, the records were taken by more professional way. Three different personal computers were used to generate the stego-image. Then, those computer transferred there resulted stego-images to another three personal computers using three different ways. The first way is by the use of mass storage - USB flash stick - to transfer the messages to the receiver terminal. The other two methods use the internet transmission, by sending the picture as an email attachment in one method, and the other method is by sending it via Skype communication or conversation.

Those three methods in transferring the Stego images ensures that, this image is valid whether it transferred directly using digital storage media, or by internet messaging. While the use of separate personal computers as receiver terminal will make some dependability of decision making for the receiver terminal program. Image security measurements that are designed to measure and analyze digital images are similarity check, correlation, histogram, and image entropy. A detection program was designed to implicitly implements those concepts and measurement methodologies. The detection program is based on trials, it uses a huge amount of trial and tries to find some meaningful result in its trials. When this result found, a hit is recorded. After that, another methodologies should be applied to extract the real message if that is possible.

In order to test the performance criteria and evaluation, a reasonable data set should be selected and tested. First, different messages have been selected to be embedded inside the images. Those messages are differ in their contents to enable testing different message sizes and their contents.

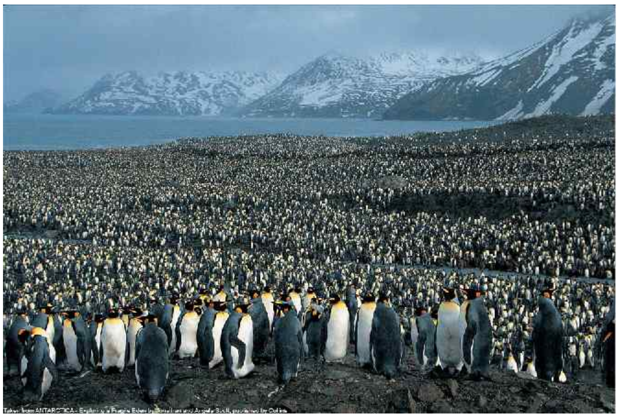
On the other hand, the carrier images, those were used in this test, are selected to be 100 images with different sizes and compression types. Some of them are gray scaled images, and most of them are RGB images. The images are randomly selected. They were collected from different locations; from windows pictures, personally taken pictures, and pictures downloaded from the internet. So, those are un-arbitrary images and mean nothing with respect to the steganography contributed algorithm.

After that, custom steganography detection program was used to detect the possibility of existence of any intrusion information inside the image. The result of this test is shown in Table I. The results were as expected, the test was not able to detect if the image contains some inconsistency or possibility to load an intrusion data. This proves the assumptions those were made along the paper. Table I shows that the test was done on different images with different compression types. This ensures that, the image is valid in any commonly used compression algorithms. The design complexity, security level, and robustness of the contributed algorithm are illustrated in the table.

Table I. Results of applying a detection program on test pattern of the stego-images

Applied Image Type	Result	No consistency percentage
.bmp	No inconsistency found	97%
.tiff	No inconsistency found	100%
.ras	No inconsistency found	99%
.ppm	No inconsistency found	95%
.hdf	No inconsistency found	100%
.png	No inconsistency found	98%

Figure 4. Un-arbitrary picture to be used as cover image



Taken from ANTARCTICA - Exploring a Fragile Eden by Jonathan and Angela Scott, published by Collins

Figure 5. The output stego-image of the covered image that was shown in figure 4

As the stego-image intended to be transferred via social media, email, messenger, memory storage, or any other image transfer technology. The most important criterion is that, it do not comprise a realistic change in comparison with the original cover image. If the stego-image distorted in a visible way, two disadvantages will be presented; first it makes the picture not reliable for common use like in social media, and second is that the picture will be subjected to some question marks. So, a good, reliable, and realistic stego-image should get negligible change in compression with the original one.

Figure (4) shows a clear cover image that is intended to add a specific message inside it. The image is from the type jpg. The resulted stego image is shown in figure (5). By human eye comparison, there is no difference between the two images. So, it passes the first test, while the statistical test that should be proved is the histogram of the two images. The histogram of the two figures (4) and (5) is shown in figure (6). Figure (a) is the original cover image histogram, whereas the figure (b) is the output image histogram result graph. It is clear from the histogram result, the input and output images are semi-identical and not easy to distinguish between them.

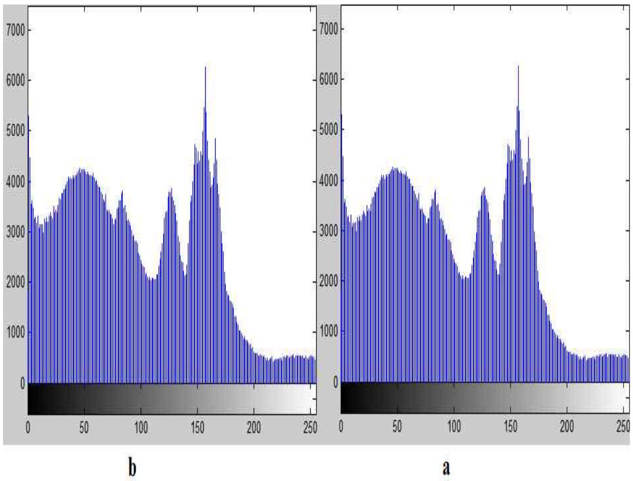


Figure 6. (a) Histogram results for the cover image and the stego-image

Table II illustrates the test results of different compression types, those are tested along the presented algorithm. The PSNR and MSE where measured for different images, and the average was recorded. The results shown in Table II are competitive and achieved high level of reliability.

Table II. PSNR and MSE measurement of the presented steganography algorithm along different compression types of images

Image Compression	**PSNR**	**MSE**
BMP	49.5111	0.7077
TIFF	49.5983	0,7133
PNG	49.0603	0.8073
PPM	49.9542	0.8111

6. Conclusion

The aim of this paper is to develop a secure steganography image algorithm that achieve a high security and high reliability through data transformation. This aim is being achieved by implementing an algorithm that message data modulation inside the wavelet domain of the cover image.

This algorithm merges both wavelet transformation and FSK modulation technique. This results a high level of information hiding and security. The high level of security presents a wall in the road of any hacking algorithm that attempts to break the stego data. Wavelet transformation is a complex transform that is not easy to deal with it statistically, especially when dealing with digitally modulated data inside that transformed signal.

The experimental results show that the stego-image is very similar to the original image, and it is not easy to be recognized even by using computer programs. In addition, the difference between the carrier and stego-image is always less than 0.1% of the image histogram difference which considered as normal image change with respect to, internet uploading, transfer media, or even compression algorithm. Thus, the presented technique combined both, security and quality.

References

[1] Feruza, Y. and Kim, T. (2007) IT Security Review: Privacy, Protection, Access Control, Assurance and System Security, International Journal of Multimedia and Ubiquitous Engineering, 2(2), 17-32.

[2] Petitcolas F.A, Anderson R.J., and Kuhn M.G. (1999). Information Hiding – A Survey, IEEE, Special Issue on Protection of Multimedia Content: 1062-1078.

[3] Atoum, M. S., Ibrahim, S., Sulong, G., Zeki, A and Abubakar, A. (2013). Exploring the Challenges of MP3 Audio Steganography. Proceding IEEE from 2nd International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Sarawak, Malaysia.

[4] Lentij J. (2000), Steganographic Methods, Department Of Control Engineering And Information Technology, Budapest University. Periodica Poltechnica Ser. El. Eng. Vol.44, No. 3–4, P. 249–258

[5] Atoum, M. S., Ibrahim, S., Sulong, G., & M-ahmad, A. (2012). MP3 Steganography: Review. Journal of Computer Science, 9(6), 236–244.

[6] Atoum, M. S., Ibrahim, S., Sulong, G., & Ahmed, A. (2013).New Secure Scheme in Audio Steganography (SSAS). Australian Journal of Basic and Applied Sciences, 7(6), 250–256.

[7] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, “Steganography and Steganalysis: different Approaches”, University of Calcutta, Kolkata, India, Tata Institute of Fundamental Research Mumbai, India, 2005.

[8] Sutaone, M.S., Khandare, M.V, “Image based steganography using LSB insertion technique”, IEEE WMMN, pp. 146-151, January 2008.

[9] Nameer N. EL-Emam, Hiding a Large Amount of Data with High Security Using Steganography Algorithm, Journal of Computer Science 3 (4): 223-232, 2007, ISSN 1549-3636, 2007 Science Publications.

[10] Debnath Bhattacharyya, Poulami Das, Bandyopadhyay, Tai-hoon Kim, Text Steganography: A Novel Approach, International Journal of Advanced Science and Technology, Vol. 3, February, 2009.

[11] Ashraf M. Emam, Mahmoud M. Ouf, Performance Evaluation of Different Universal Steganalysis Techniques in JPG Files, Annales UMCS Informatica AI XII, 3 (2012) 121–139 DOI: 10.2478/v10065-012-0026-y.

[12] Davidson, J. and Bergman, C. and Bartlett, E. An artificial neural network for wavelet steganalysis, Proceedings of SPIE - The International Society for Optical Engineering, Mathematical Methods in Pattern and Image Analysis, vol. 5916, pp. 1-10. ISBN 0-8194-5921-6, August 2005, San Diego, California, USA.

[13] Rosziati Ibrahim and Teoh Suk Kuan, Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Application 2 (2011) 102-108.

[14] Anjali A. Shejul, Umesh L. Kulkarni, A Secure Skin Tone based Steganography Using Wavelet Transform, International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011 1793-8201.

[15] J.K. Mandal, Madhumita Sengupta, Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC), 2010 International Symposium on Electronic System Design.

[16] Ali Al-Ataby and Fawzi Al-Naima, A Modified High Capacity Image Steganography Technique Based on Wavelet Transform, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[17] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm, Proceedings of the International MultiConference of Engineers and Computer Scientists 2011 Vol1, IMECS 2011, March 16 - 18, 2011, Hong Kong.

[18] Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.