ILSB: Indexing with Least Significant Bit Algorithm for Effective Data Hiding

A. N. Senarathne
Sri Lanka Institute of
Information Technology
New Kandy Road,
Malabe, Sri Lanka

Kasun De Zoysa
University of Colombo
School of Computing
University of Colombo
Sri Lanka

ABSTRACT

Data transmission is frequently face intrusions issues. Different data hiding methods are there to address this problem. Steganography being one; intends on writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Moreover, cryptography is a tool used in protecting information using cipher text. However, these methods are subjected to suspicion and prone to visual and statistical attacks. While trying to overcome such problems, researchers need to compromise with imperceptibility and hiding capacity. Any basic algorithms including traditional Least Significant Bit algorithm are simpler and faster processing although they are highly vulnerable to these visual and statistical attacks. Once the algorithm is known extracting the hidden information is fairly simple using steganalysis tools. Thus, these are having relatively low data hiding capacity, security compared to the algorithms with enhancements. These enhancements use complex mathematical functions with existing algorithms using cryptography as a method of improving security. The employing cryptography involves complex mathematical calculations requiring advanced processing capabilities leading to slow performance. As a result; it's difficult to work in low processing environments.

This research focuses on developing a system that adapts to the enhanced security without using complex mathematical functions with ways in which to improve data hiding capacity. Having less complexity intern provides the user with lower processing environment. The system uses an indexing technique in hiding data inside the cover image providing high security. The proposed system will have an additional step residing outside the traditional Least Significant Bit algorithm which provides hiding data with less vulnerability to intrusion. The requirement of an indexing image will provide the user with high security because the extraction process will totally depend on the bit patterns of the indexing image. This enhancement will be an attempt to overcome threats and weaknesses in the traditional Least Significant Bit algorithm and enhance the security of data hiding.

Keywords

Indexed Least Significant Bit, Information security, Steganography, Data Hiding, Intrusion prevention

1. INTRODUCTION

Data transmission is constantly subjected to intrusions. Numerous data hiding methods have been developed and employed to address the above. Steganography being once; is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspect the existence of the message, a form of security through obscurity [1]. On the other hand, cryptography is an indispensable tool for protecting information in computer systems. While cipher text created using cryptographic mechanisms might arouse suspicion; the invisible messages created with steganographic methods are prone to visual and statistical attacks [2], [3], [4], [5]. The human eye is skilled in identifying the known patterns. This human ability is the basis for the visual attacks [3]. In the meantime, the traditional least significant bit (LSB) algorithm uses a fixed set of Pairs of Values (PoVs) to flip each other while embedding message bits. This attracts statistical attacks. Moreover, swapping one value into another does not change the sum of occurrences of both colours in the image; therefore, it can be used in designing a statistical Chi-square test [4]. However; its imperceptibility and hiding capacity are relatively low [6]. This is mainly because the significant bits of the secret message are hidden in the cover medium in a linear and deterministic pattern. Retrieval of secret data using steganalysis software tools therefore becomes relatively easy once the algorithm used is known. Any basic algorithm including traditional LSB are simpler and faster processing although they are highly vulnerable to these visual and statistical attacks [7]. Thus, these are having relatively low data hiding capacity compared to the algorithms with enhancements. Most of these enhancements use cryptography as the means of improving security. Hence, the complexity of the algorithm increase and these complex mathematical functions used while enhancing are in need of high processing capacity. As a result; it's difficult to work in low processing environments [6]. The systems emphasis on security uses algorithms such as RC4, pseudo random number generators, key permutation methods, Rivest, Shamir, Adleman (RSA) and Diffie Hellman in the encryption process [29], [30], [31], [32].

2. LITERATURE REVIEW

Least significant bit (LSB) algorithm being one of the simple approaches in embedding messages into images uses a substitution process to adjust the least significant bit pixels of the carrier image [8]. In the meantime, there are other algorithms such as hide and seek [9], JSTEG [10], [9] and patchwork [1]. However, all of these are having the problem of embedding large amount of data without being detected and vulnerable to visual and statistical attacks [1]. There are many steganographic tools developed based on these algorithms. Which falls under two domains; namely: "spatial domain" that replaces or change pixel values and "transform domain" that manipulates the transform domain coefficients [11]. Most of the open source software as well as proprietary software available are using spatial domain algorithms such as LSB (e.g.: Blindside, Camera Shy, Hide4PGP, JP Hide and Seek, Jsteg Jpeg, Mandelsteg, Steghide, wbStego) [11]. Any basic algorithm including traditional LSB is simpler and faster processing. Once the algorithm is known; retrieving secret data using steganalysis software tools are relatively easy [7]. To overcome this; the amount of data being embedded using traditional algorithms are kept relatively low compared to the algorithms with enhancements. Prior research shows that there is an enhanced LSB method using LSB to embed information within an encrypted image data randomly [12]. This method spreads hidden information within encrypted image data randomly based on the secret key before transmission. Nevertheless; this only reduces the chance of the encrypted image being detected to enhance the security level of the encrypted images. Moreover; a another system proposed using advanced LSB embedding scheme which breaks the regular pattern of PoVs in the histogram domain, increasing the difficulty of steganalysis and thereby raising the level of security [13]. However, the increasing amount of data embedded in the image is not a consideration in this research. Another proposed enhanced LSB method uses a genetic algorithm with LSB [14]. Once embedding the secret message in LSB of the cover image, the pixel values of the Stego image are modified by the genetic algorithm to keep their statistic characters. Thus, the existence of the secret message is hard to detect except increasing amount of data embedded in the image is not considered while enhancing. SLSB (Selected Least Significant Bit) is another proposed method which improves the performance of the LSB method by hiding information only in one of the three colours at each pixel of the cover image [7]. Doing this will only reduce the chance of the hidden data being detected. Another proposed method increases the level of imperceptibility and the hiding capacity in the LSB insertion method; an enhanced LSB method that employs a selective and randomized approach in picking specific number of target image bits to swap with the secret data bits during the embedding process [6]. To facilitate the selective picking of the target image bits, the standard minimal linear congruential number generator (LCG) is used. The message digest (digital signature) of a user supplied password is used to seed the LCG and to extract the message from the cover medium. However; the complexity is the drawback in proposed method. The overall complexity associated with the existing algorithms while enhancing is leading to slowness and need more processing which makes it difficult to work in low processing environments [6]. Most of these have focused on improving the traditional LSB algorithm (e.g.: [12], [15], [7], [16]). Prior research on enhancements to traditional LSB is described in the coming topics.

2.1 Selective and randomized approach in picking specific number of target image bits

The traditional LSB algorithm is simple and its imperceptibility and hiding capacity are relatively low. Therefore; the statistical characteristics of its resultant stego images are revealed. Hence, this research proposes an enhanced LSB method that employs a selective and randomized approach in picking specific number of target image bits to swap with the secret data bits during the embedding process. To facilitate the selective picking of the target image bits, the standard minimal linear congruential number generator (LCG) is used. The message digest (digital signature) of a user supplied password is used to seed the LCG and to extract the message from the cover medium. The effectiveness of the method is measured by using an experimental research design where the statistical characteristics of the proposed method stego images were compared with those of the traditional LSB method in a comparative experiment designed to establish the levels of image distortion (noise) introduced in the original cover image when either of the methods is used under the same payload and image. The experiment results indicated improved levels of imperceptibility and hiding capacity in the method.

In comparison to the traditional least significant bit algorithm, the data hiding steganographic method presented was found to demonstrate increased imperceptibility to statistical steganalysis attacks on the cover image. The hiding capacity can also be increased by varying the number of bits used per colour channel. However, this method is best suited for the purposes of communication and communication applications as more permanent aspects of steganography like watermarking are not included.

Similar to other steganographic applications, the cover images used should be high quality original photographs. There commended mode of transmission of the stego images is through web postings or email attachments. Since; digital steganography is a rapidly growing and increasingly interesting field of research for information hiding and data security. It is currently playing a vitally important role in defense and civil applications. Researchers encourage future work on data security applications based on this technology with stronger embedding algorithms whose output can survive image manipulations and those that can make use of more permanent embedding procedures. This will facilitate the use of steganography in more sensitive application areas like in computer digital forensics and in enhancement of security in electronic commerce and trading applications. Research along these lines will also help in ensuring a permanent solution to the issues of plagiarism of copy write digital content materials [12].

2.2 Selected Least Significant Bit method

This research presents a steganographic algorithm based on the spatial domain. The least significant bits of one of the pixel colour components in the image and change them according to the message’s bits to hide. The rest of bits in the pixel colour component selected are also changed in order get the nearest colour to the original one in the scale of colours. This method was compared with others that work in the spatial domain and the great difference is the fact that the LSBs bits of every pixel colour component are not used to embed the message, just those from pixel colour component selected.

The system uses a Sample Pairs analysis prior to steganography, which allows the selection of the best colour of the three possible to hide information. Further it uses a pixel selection filter to obtain the best areas to hide information. By using implement, the LSB Match method to reduce the difference between the original pixel and the steganographic pixel; the system provides immunity against visuals attacks. Changes are undetectable with the naked eye, and a filter of LSB bits doesn’t present areas of random information that could indicate the presence of hidden information. Further it is immune to attacks by comparing histograms, as the frequency of appearance of colours in the steganographic image is very similar to that of the cover image. Moreover, it is immune to statistical attacks, as two colours for each pixel are equal to those of the original image, and the final ratio of analysis is very close to the original image, which doesn’t raise suspicion it contains hidden information. Even in some cases get better rates than those of the original image, creating confusion over which of two images would be the original. Researchers propose future work on achieving better performance and be undetectable by the most famous steganographic analysis, for example, changing bits undisturbed by the concealment of the message [7].

2.3 LSB to embed information within an encrypted image randomly

This approach uses the Least Significant Bits (LSB) insertion to hide data within encrypted image data. The binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. Experimental results show that the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy have not changed, the method offers a good concealment for data in the encrypted image, and reduces the chance of the encrypted image being detected. The hidden data will be used to enable the receiver to reconstruct the same secret transformation table after extracting it and hence the original image can be reproduced by the inverse of the transformation and encryption processes. Thus, it will be used to reduce the chance of the encrypted image being detected and then enhance the security level of the encrypted images [12].

2.4 Advanced LSB through breaks the regular pattern of PoVs in the histogram domain

This research also identifies LSB steganographic data embedding is simple to understand, easy to implement, and it results in stegoimages that contain hidden data yet appear to be of high visual fidelity. However, it can be shown that under certain conditions, LSB embedding is not secure at all. The research focus on a fatal drawback of LSB embedding is the existence of detectable artifacts in the form of pairs of values (PoVs). Hence goals of the research are to present a theoretic analysis of PoVs and to propose an advanced LSB embedding scheme that possesses the advantages of LSB embedding suggested above, but which also provides an additional level of communication security. It breaks the regular pattern of PoVs in the histogram domain, increasing the difficulty of steganalysis and thereby raising the level of security. The experimental results of the research show that both the Chi-square index and RS index are less than 0.1,.There are three important features within the modified scheme. Firstly, the extraction process used in the proposed scheme is almost identical to the one used in traditional LSB embedding. Secondly, from a PSNR point of view, the fidelity of the stego images resulting from the proposed scheme is as good as those created by traditional LSB embedding. Finally, and most importantly, the PoVs artifact is removed from the stego-images [13].

2.5 A genetic algorithm with LSB

This research also focuses on LSB encoding; which is the simplest encoding method used by many steganography programs to hide secret message in 24bit, 8bit colour images and grayscale images. Steganalysis is a method of detecting secret message hidden in a cover media using steganography. RS steganalysis is one of the most reliable steganalysis which performs statistical analysis of the pixels to successfully detect the hidden message in an image. However, existing steganography method protects the information against RS steganalysis in grey scale images. This research presents a steganography method using genetic algorithm to protect against the RS attack in colour images. Stego image is divided into number of blocks. Subsequently, with the implementation of natural evolution on the stego image using genetic algorithm enables to achieve optimized security and image quality. Nevertheless, as the length of the secret message increases, the probability of detection of secret message by RS analysis also increases. However, our future work focus upon the improvement in embedding capacity and further improvement in the efficiency of this method [14].

2.6 LSB enhancements with cryptography

As discussed above there are different enhancements made on traditional LSB to improve its data hiding capacity. Further there are improvements made on the security of the secrete message. In doing so cryptography related encryption stands out [29], [30], [31], [32]. Prior research emphasis on such improvements made based on cryptography. One such uses LSB based data embedding technique to hide the encrypted message in digital systems. However before embedding the secret message, RC4 algorithm is also used for message encryption. Further it uses Pseudo Random Number Generator in generating the random sequences in order to hide the secret messages within PNG image file using random sequences [29]. Another technique on internet steganography focuses on digital watermarking. This is based on the LSB algorithm and a new encryption algorithm which matches data to an image with the objective of lesser chance of an attacker being able to use steganalysis to recover data. Before hiding the secrete message in an image the application first encrypts the message to be sent using this new algorithm [30]. Moreover, there are other methods using hybrid data hiding scheme incorporating LSB algorithm with a key-permutation method. The objective was to propose an optimal key permutation method using genetic algorithms for best key selection. The results show decrement in computation time when increasing number of keys, at the same time system security improves [31]. Another previous research is focusing on information security in a low cost environment by using encryption techniques such as Rivest, Shamir, Adleman (RSA) algorithm and Diffie Hellman algorithm to encrypt the data [32].

3. RESEARCH OBJECTIVES

The objective of this project is to develop an enhancement to traditional LSB with improved security with data hiding capacity in a lower processing environment. This approach contains minimal amount of modifications to the cover image whilst embedding data. Hence, the system is expected to withstand against visual and statistical attacks without creating suspensions to third parties while providing its services to high level of security with improved capacity of data hiding than traditional LSB without adding high complexity or high processing activities associated with existing enhancements.

Sub objectives of this project are:

- To develop the enhancements as an separate individual component works with traditional LSB in a way the same concept can be used irrespective of the algorithm (traditional or enhanced) and file format

- To develop the enchantment in a way to provide additional layer of security against extracting data than traditional LSB in case of a threat or an attack

- To find suitable parameters to measure the enhancement against traditional LSB and compare this enhancement with traditional LSB with enhancements and other techniques using several rounds of compression

4. RESEARCH METHODOLOGY

The methodology covers the basic concepts used in this research. Each subtopic will cover the justification of the research methodology.

4.1 Steganography

Steganography comes from the Greek words steganos or "covered," and graphie, or "writing" [20]. It is the process of hiding a secret message within an ordinary message and the extraction of it at its destination. The goal is to hide the presence of a message within another message by using it as the cover. Therefore, depending on the cover medium different type of steganography techniques are available such as; Text Steganography, Image Steganography, Audio Steganography and Video Steganography [18].

Out of these most commonly used is the image steganography [23]. There are four distinctive elements in Steganography. Those are the cover medium, the secret message, the stego-object and the stego-key [19]. These are described below.

4.1.1 The Cover

Steganography uses a cover medium to hide the secret data. It is a crucial part of steganography since the effectiveness of the steganographic technique is dependent on it. If suspected of a hidden message it could result in exposing. When the cover medium is innocent and harmless the result of exposure is minimal. Therefore, images are being used more often as cover medium. However; the images used as covers contain certain properties which allow hiding large amount of data without any visual distortion. Hence, images with fewer colours are bound to be more suspicious than images with various colours.

4.1.2 The Secret Message

The message must be serializable, so that it may be embedded bit by bit into the cover. Further it must be smaller than the cover. Having larger messages will make the steganography process less effective. More often the exchanged secret messages are in form of text.

4.1.3 Stego Object

The stego objects are created when the secret message is embedded within the cover. In image steganography this is referred as a stego image.

4.1.4 Stego Key

In order to retrieve the original secret message; receiver needs to know the key used in the embedding process. At present there are many algorithms developed and improved for embedding and extracting process. In almost all the cases where the stego key is used it comes with cryptographic process to encrypt data which lead to a high processing environment with complex mathematical functions.

4.2 Steganography

Image steganography uses an image as the cover medium. This is the widely used cover medium [23]. There are different algorithms in order to hide a message within an image.

4.2.1 An Image

An image consists of numeric representations of distinctive light intensities forming a grid. The individual points on the grid are referred to as pixels. Within the image these pixels are displayed horizontally row by row. The number of bits used for each pixel is called bit depth which represents the number of bits in a colour scheme. The smallest bit depth (bits representing a pixel) in current colour schemes is 8. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colouris represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours [1], [22].

There are different types of image file formats used in steganography, namely; BMP, JPEG, TIFF, GIF and PNG [18]. In available steganography tools; the most popularly used cover image type is BMP [11]. This research focuses on using BMP image file format.

4.2.2 Bitmap images (BMP)

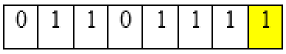
BMP was introduced by Microsoft as a standard image file format for Widows OS also known as bitmap. This format is supported across multiple file systems and operating systems. When comes to embedding secret messages; having large file size is an advantage because having this characteristic will not raise suspicion [21]. General BMP properties are as follows:

- A bitmap format that can be uncompressed, or compressed with RLE
- BMP files are;
    - In 1-bit black and white.
    - 8-bit grey scale.
    - 16-, 24- or 32-bit RGB colour.
    - or 4- or 8-bit indexed colour .
- BMP files don't support CMYK colour.
- Transparency is supported for individual pixels as in GIF files.
- Alpha channels are supported in new versions of BMP.

Since indexed colour images consists of compressed colours; the images with high bit depth are more suitable in image steganography. The 24 bit images can represent each colour in RGB with one Byte containing 8 bits.

4.3 LSB Algorithm

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [1]. The 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message.



0	1	1	0	1	1	1	1

Fig 1: Least significant bit

A BMP is capable of hiding quite a large message. LSB in BMP is most suitable for applications, where the focus is on the amount of information to be transmitted [18]. But with the LSB the main objective of Steganography is to pass a message to a receiver without an intruder even knowing that a message is being passed is being achieved. Prior researches have compared the effectiveness of LSB in both BMP and JPEG file format in performing image steganography using following parameters:

- Invisibility– The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised

- Payload capacity–Unlike water marking, which needs to embed only a small amount of copyright in formation, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

- Robustness against statistical attacks–Statistical steganalysis is the practice of detecting hidden information through applying statistical test son image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

- Robustness against image manipulation– In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

- Independent of file format–With many different image file formats used on the Internet, It might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed in formation in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

- Unsuspicious files–This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

When embedding a message in a "raw" image that has not been changed with compression, such as a BMP, there exists a trade-off between the invisibility of the message and the amount of information that can be embedded. A BMP is capable of hiding quite a large message, but the fact that more bits are altered results in a larger possibility that the altered bits can be seen with the human eye. Suggested application of LSB in BMP is most suitable for applications where the focus is on the amount of information to be transmitted and are indexed component of the implementation provides with an additional layer of security for the information hidden.

5. RESEARCH DESIGN

This research implements the indexed LSB (ILSB) algorithm. This is to provide a layer of security to the hidden image and LSB will create a low processing environment. Once the ILSB is completed a rigorous testing process will be carried against the traditional LSB. The following subsections will cover the design of the ILSB.

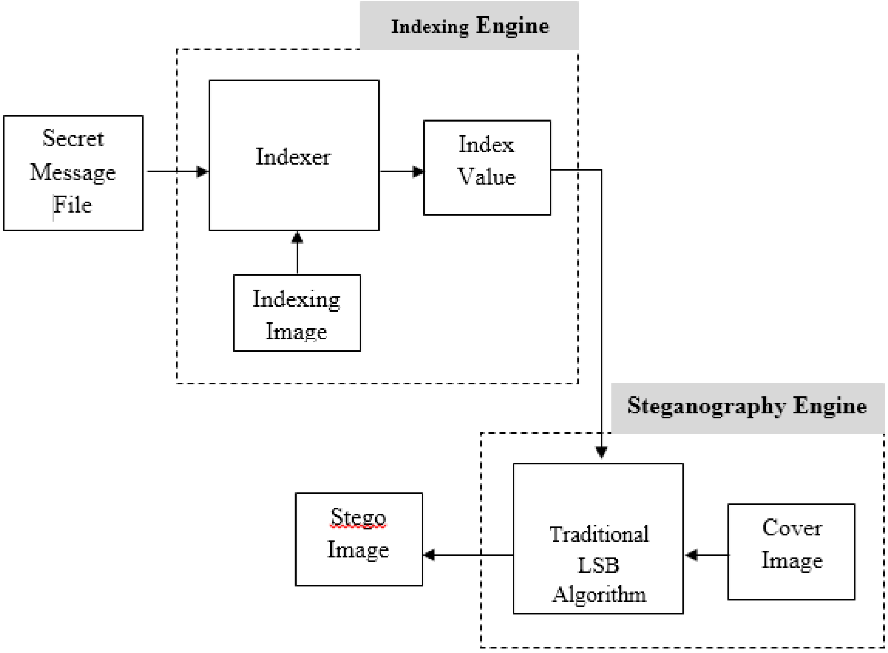


Fig 2: Design of ILSB embedding process

5.1 Design of Indexed LSB embedding process

The above indexed LSB design illustrates the overall design of the proposed development. There are two components in this implementation. First, the indexing engine which is used to generate an index with the use of a secrete message and an image. Once generated; the index will be embedded on a cover image with the traditional LSB algorithm to generate the stego image inside the steganography engine. Both indexer engine and the steganography engine is illustrated and explained in the next two subsections.

5.1.1 Indexer Engine

As depicted below the indexer engine consists of two parts. First, both the secrete message file and the image (indexing image) used as the base for finding the index will be converted into two separate Byte arrays.

Once converted; the Bytes of the indexing image will convert into an array of unique bit patterns by eliminating the repetitive patterns. Since all of these are of 8 bits the maximum number of patterns will be of 0 to 255. However, the order of the patterns will be dependent on the image used in indexing. The sender has the capability to choose any image as the indexing image. Once the unique patterns are identified; the Byte array of the message will be compared against the unique patterns. The matching values will be stored in a list of pre-index values. This list contains all the pre-index values available for the secrete message within the indexing image. Then the pre-index will be substituted by predefined values of the substitution table. The values containing the substitution table will be represented in the implementation stage.

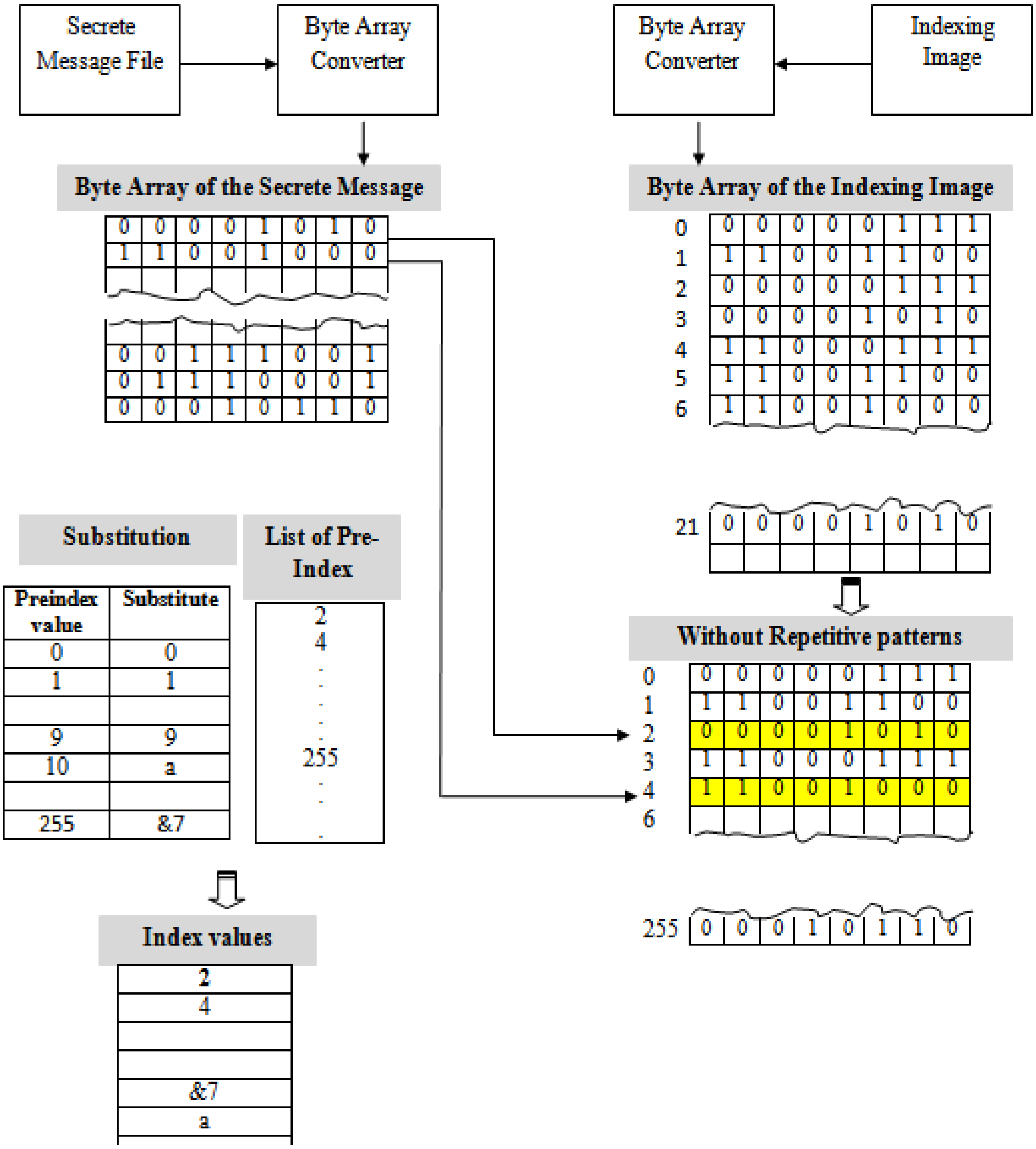


Fig 3: Indexer Engine

5.1.2 Steganography Engine

As illustrated below the steganography engine will be taking a cover image and the list of index values generated by the indexer engine as the inputs. The list of index values will be converted to a Byre array.

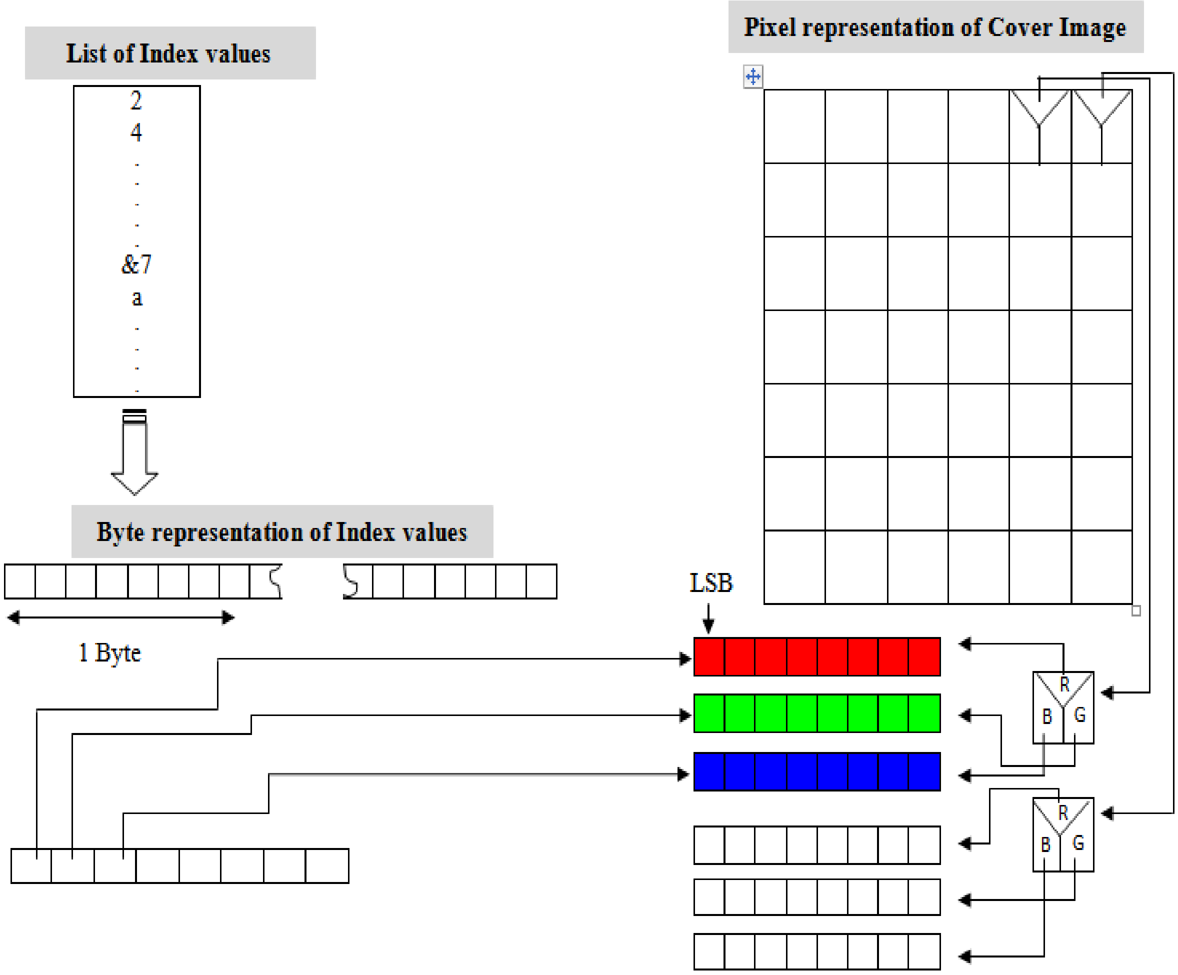

List of Index values
2
4
&7
a
Byte representation of Index values
1 Byte
Pixel representation of Cover Image
LSB
R
B
G
R
B
G

Fig 4: Steganography Engine

Since each pixel within the cover image consists of 3 colour representing red, green and blue; each colour is represented in term of one byte. The bite representation of the list of index values will be embedded within the 8th or the least significant bit of the each colour within a given pixel. This is done with the use of traditional LSB algorithm.

5.2 Design of Indexed LSB extracting process

The below indexed LSB design extracting process illustrates the overall design of the extracting process of the proposed development. There are two components in this implementation. First, the index extracting engine which is used to generate an index vale from the stego image; next the message extracting engine which is used in extracting the secrete message from the index. Since the traditional LSB is used in this development there is a chance of an intruder identifying the stego image and performing a search on extracting the message. However, the presence of the index will be a limitation because the hidden message can only be extracted with the availability of the image used in generating the index file. Therefore, the index will present an additional layer of security by being a key for the message extraction process.

5.2.1 Index Extracting Engine

When the stego image is input to the index extraction engine; each pixel will be broken down in to the three bytes representing red, green and blue. Then the traditional LSB extraction process will be used in order to generate the bit representation of the index values.

5.2.2 Message Extracting Engine

At the message extracting engine; the indexing image will be used as a decoder for the index values extracted from the index extracting engine. Therefore; the indexing image will be acting as a key between the sender and the receiver. Once identified the matching bi patterns the original message byte array will be generated and converted back to the original secrete message.

6. RESULTS AND DISCUSSION

To be able to compare the performance of this improvement on the LSB method, several images will be used as cover with BMP (Bit Mapped Picture) format and 512x512 pixels in size with file size of 768 KB (786,486 Bytes) with bit depth of 24 bits/pixel.

Further analysis will be performed with the use of 256x256 pixels BMP images with bit depth of 24 bits/pixel.

6.1 Images used in the evaluation process

All the experiments were implemented with the following constants:

- Same images were used on all methods (both traditional LSB and Indexed LSB)
- Same information was embedded in each image
- Same evaluation metrics were used for each image
- Five digital images were used as test data files (cover images).

Fig 5: Baboon.bmp

Fig 6: Lena.bmp

Fig 7: Sailboat.bmp

Fig 8: F16.bmp

Fig 9: Peppers.bmp

6.2 Measurements used in evaluation

There are several measurements used in evaluating the images generated from ILSB. These will be used against images generated from ILSB, traditional LSB and steganography tools using LSB. The measurements are Universal Image Quality Index (UQI), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), Structural Similarity Index (SSIM) and Mean Structural Similarity Index (MSSIM), Noise Quality Measure (NQM), Visual Information Fidelity (VIF) and Signal to Noise Ratio (SNR) and Weighted Signal to Noise Ratio (WSNR).

Above mentioned measures of distortion (Structural Similarity Index, Multi-scale SSIM Index (MSSIM), Noise Quality Measure (NQM), Universal Image Quality Index (UQI), Visual Information Fidelity (VIF), Signal-to-Noise Ratio (SNR, PSNR)) applied to steganographic images obtained by original image, stego image of LSB and stego image of ILSB. A lower distortion represents a better steganographic method because it is closer to the values of the original image.

6.3 Results of the evaluation

For the ISLB steganography both the indexing image and the cover image are the same. Moreover; the hidden message is having a file size of 9.39 KB (9,618 bytes) for testing purposes. The results represent the values obtained using the original image, ISLB and traditional LSB. The results obtained using the images mentioned above are shown below:

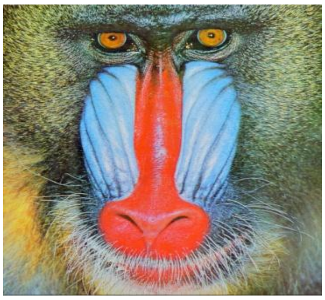
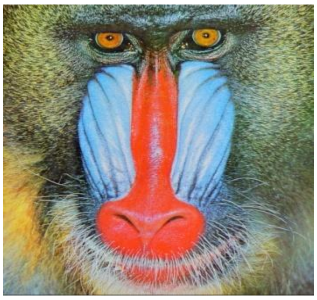
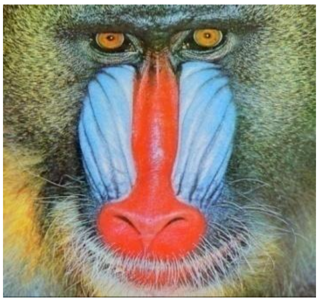
6.3.1 Images with 512x512 pixels

Table 1: Test results of 512x512 Lena.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99925	64.8335	0.99978	68.6785	57.14583	0.99836	0.02137	48.71268
c	0.99944	66.28096	0.99984	71.50769	58.59328	0.99882	0.01531	52.87528

Table 2: Test results of 512x512 Baboon.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**
		

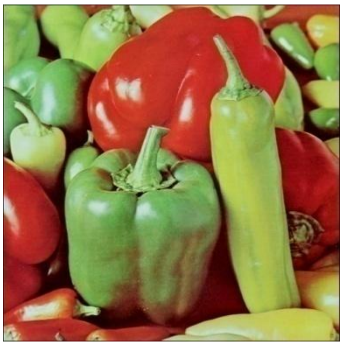
#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99998	64.80852	0.99998	70.61905	59.37062	0.99875	0.02149	45.71998
c	0.99999	66.16496	0.99999	73.59054	60.72706	0.99908	0.01572	49.83247

Table 3: Test results of 512x512 F-16.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**

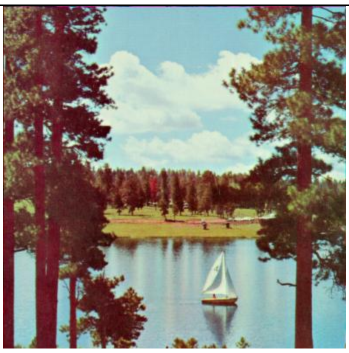
#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99926	64.7971	0.9998	73.63378	62.01414	0.99832	0.02155	45.35135
c	0.99954	66.17322	0.99986	76.33418	63.39027	0.99876	0.01569	48.4824

Table 4: Test results of 512x512 Peppers.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**
		

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99935	64.73678	0.99984	70.2501	58.77878	0.99838	0.02185	51.94251
c	0.99956	66.06699	0.99989	72.58534	60.10899	0.99879	0.01608	57.43055

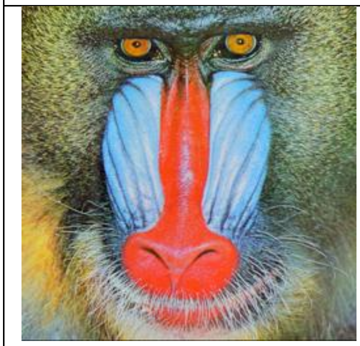
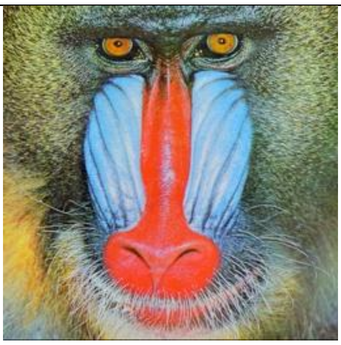
Table 5: Test results of 512x512 Sailboat.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**
		

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99954	64.74236	0.99988	71.10979	59.61844	0.99864	0.02182	50.92262
c	0.9997	66.19409	0.99992	73.45849	61.07017	0.99899	0.01562	55.60223

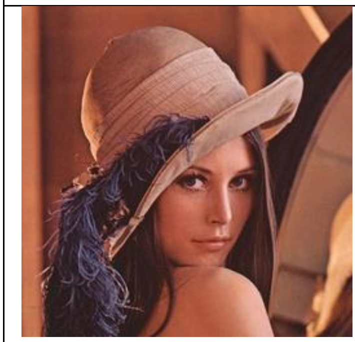
6.3.2 Images with 256x256 pixels

Table 6: Test results of 256x256 Baboon.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**
		

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99982	58.75692	0.99985	64.88493	53.25047	0.99489	0.08657	42.48126
c	0.99992	60.06684	0.99992	67.54936	54.56039	0.99616	0.06403	43.74356

Table 7: Test results of 256x256 Lena.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**
		

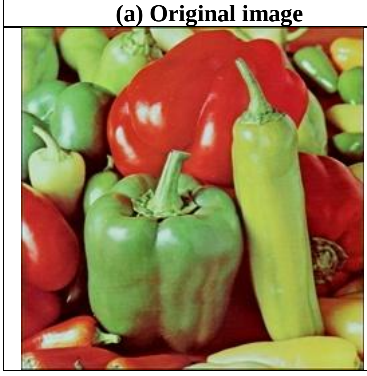
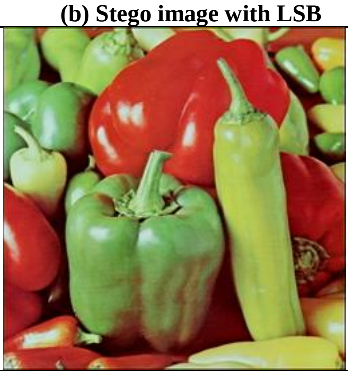
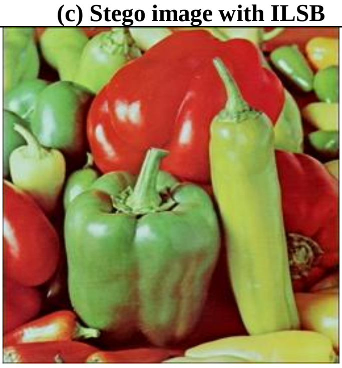
#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99692	58.74602	0.99931	62.48841	51.04663	0.99406	0.08679	46.04078
c	0.99761	60.20255	0.99945	65.40216	52.50316	0.99575	0.06206	47.49034

Table 8: Test results of 256x256 F-16.bmp

(a) Original image	**(b) Stego image with LSB**	**(c) Stego image with ILSB**

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99561	58.77557	0.9991	67.65265	55.98999	0.99441	0.0862	40.57674
c	0.99723	60.29464	0.99937	70.30433	57.50906	0.99592	0.06076	42.39919

Table 9: Test results of 256x256 Peppers.bmp

(a) Original image	(b) Stego image with LSB	(c) Stego image with ILSB
		

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99819	58.75242	0.99952	64.18698	52.78266	0.99478	0.08666	48.28251
c	0.99856	60.2748	0.99965	66.95106	54.30504	0.99635	0.06104	50.57584

Table 10: Test results of 256x256 Sailboat.bmp

(a) Original image	(b) Stego image with LSB	(c) Stego image with ILSB

#	UQI	PSNR	SSIM	WSNR	SNR	PBVIF	MSE	NQM
a	1	Inf	1	Inf	inf	1	0	inf
b	0.99595	58.7563	0.99954	65.15195	53.62131	0.99519	0.08659	46.75737
c	0.99662	60.29259	0.99967	68.06929	55.1576	0.99664	0.06079	48.20033

7. CONCLUSION

Data transmissions across networks are always subjected with issues relating to intrusion. The methods used in improving security are having complex algorithms relating to cryptography and encryption. These are having highly complex mathematical functions requiring high processing capabilities. On the other hand, the once who tries to achieve high data hiding capacity struggles with exposing to third parties. There are different mechanisms employed in order to overcome these issues. However, there are always compromises with one when the other is improved. This research focuses on finding a steganography solution that tries to enhance the traditional LSB algorithm with additional security layer provided by indexing. Further this will try to strike a balance between security, data capacity and complexity.

This new method Indexed Least Significant Bit (ILSB) is expected to improve the security of the traditional LSB algorithm while improving data hiding capacity in the cover image in a lower processing environment. An index will be generated prior to the embedding process.

The newly developed enhancement is having the following capabilities. Improve security of the traditional LSB by adding additional security layer and improve performance in low processing environments. Since the enhancement is implemented in a way to create the index depending on the index image used to the process. Once the byte array of the index image is created without repetitive patterns, order of all

256 elements in that array is depends on the index image. The value 256 comes with the number of unique patterns can be found while representing 8 bits. Therefore, the final index used to hide inside the cover image as data is depending on the index image. Generation of the original index to generate the original message is only possible if the input is the same index image. In case of a Brute-force attempt to create the byte array of the index image with all 256 elements in the same order have test values of factorial 256 (value of 256! is equal to 8.5781777534284265411908227168123e+506). It confirms that this method provides an advance level of security without adding a cryptographic process and use of a user input key. In ILSB the index image itself is acting as the key to the process. Eventually this will lead to following benefits:

- User has no overhead of inserting a secure key to the embedding and extraction process.
- No need to have secure ways to exchange the keys between sender and the receiver. It is just a matter of exchanging the index image through a public or private media without getting noticed.
- No overhead of remembering or storing the key on sender or receiver side.
- No complex mathematical computations implemented such as cryptographic functions which lead to low processing.

Furthermore, any improvements in capability of hiding capacity with less vulnerability to visual and statistical will itself provide security to protect the index hidden in the stego image using traditional LSB.

Since there are no complex mathematical functions used in this apart from indexing; there is no drastic improvement in the data hiding capacity in ILSB. However, the modern steganography tools achieve high data capacity by applying several rounds of high processing compression algorithms therefore this provides a platform for the developers to apply those compressions effectively with the message as well as with the index resulting in improving data hiding capacity of tools to be developed using ILSB.

8. FUTURE WORK

At present the enhancement work in BMP; to achieve independence of file formats requires the enhancement to work in most of the image file formats available. In order to optimize the data hiding capacity the indexing algorithm should be improved.

9. REFERENCES

[1] N. F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998

[2] N. Provos and P. Honeyman, “Detecting Steganographic Content on the Internet”, Center for Information Technology Integration, University of Michigan, August 2001

[3] A. Westfeldand and A. Pfitzmann, “Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned”, Dresden University of Technology, Department of Computer Science, Germany

[4] J. Fridrich and M. Goljan, “Practical Steganalysis of Digital Images – State of the Art”, SUNY Binghamton, Department of Electrical Engineering, Binghamton

[5] N. N. EL-Emam, “Hiding a Large Amount of Data with High Security Using Steganography Algorithm”, Journal of Computer Science, Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan, 2007

[6] G. M. Kamau, S. Kimani and W. Mwangi, “An enhanced Least Significant Bit Steganographic Method for Information Hiding”, Journal of Information Engineering and Applications, Vol 2, No.9, 2012

[7] J. J. Roque and J. M. Minguet, “SLSB: Improving the Steganographic Algorithm LSB”, Universidad Nacional de Educación a Distancia (Spain)

[8] C. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution”, The Journal of Pattern Recognition Society, Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong, 2003

[9] L. M. Marvel, C. G. Boncelet Jr and C. Retter, “Spread Spectrum Steganography”, IEEE Transactions on image processing, 8:08, 1999

[10] S. K. Muttoo and S. Kumar, “Data Hiding in JPEG Images”, BVICAM’S International Journal of Information Technology, BharatiVidyapeeth’s Institute of Computer Applications and Management, New Delhi, 2008

[11] P. Hayati, V. Potdar and E. Chang, “A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator”, Institute for Advanced Studies in Basic Science of Zanjan, Iran

[12] M. A. B. Younes and A. Jantan, “A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion”, International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008

[13] Y. K. Lee, G. Bell, S. Y. Huang, R. Z. Wang and S. J. Shyu, “An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding” in Advances in Image and Video Technology, vol. 5414, Berlin, Heidelberg: Springer, 2009, pp. 349-360.

[14] S. Wang, B. Yang and X. Niu, “A Secure Steganography Method based on Genetic Algorithm”, Journal of Information Hiding and Multimedia Signal Processing, VOL.1 No.8, January 2010

[15] A. D. Ker, “Improved Detection of LSB Steganography in Grayscale Images” Oxford University Computing Laboratory, Parks Road, Oxford OX1 3QD, England, 2004

[16] X. Zhang and S. Wang, “Efficient Steganographic Embedding by Exploiting Modification Direction”, IEEE COMMUNICATIONS LETTERS, VOL. 10, NO. 11, NOVEMBER 2006

[17] S. Katzenbeisser and F. Petitcolas, “Information hiding techniques for steganography and digital watermarking.”,Artech House Books, 1999. [18] E. E. Elgabar, “Comparison of LSB Steganography in BMP and JPEG Images”,International Journal of Soft Computing and Engineering ,pp.91-95.2013.

[18] A. Miller,“LEAST SIGNIFICANT BIT EMBEDDINGS:IMPLEMENTATION AND

DETECTION". Retrieved December 22, 2013, from aaronmiller.in: aaronmiller.in/thesis, 2012, May

[19] T. Moerland, "Steganography and Steganalysis". 2003, Retrieved December 23, 2013, from www.liacs.nl/home/ tmoerl/privtech.pdf

[20] MSDN:About Bitmaps. 2007. Retrieved December 22, 2013, from M Corporation: <http://msdn.microsoft.com/library/default.asp?url=/library/enus/gdi/bitmaps_99ir.asp?frame=tru

[21] M. O. Owens, "A discussion of covert channels and steganography".SANS Institute.2002

[22] M. S. Rana, B. S. Sangwan and J. S. Jangir, "Art of Hiding: An Introduction to Steganography",International Journal Of Engineering And Computer Science ,Vol.1 I. 1, pp:11-22.

[23] Z. Wang, H. R. Sheikh and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images". Proceedings of the International Conference on Image Processing,2002, Vol.1,pp. 477-480.

[24] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity" IEEE Transactions on Image Processing, vol. 13, no. 4, pp.600-612, Apr. 2004

[25] H. R. Sheikh and A. C. Bovik, "Image Information and Visual Quality"., IEEE Transactions on Image Processing.

[26] J. Mannos and D. Sakrison, "The effects of a visual fidelity criterion on the encoding of images", IEEE Trans. Inf. Theory, IT-20(4), pp. 525-535, July 1974.

[27] T. Mitsa and K. Varkur, "Evaluation of contrast sensitivity functions for the formulation of quality measures incorporated in halftoning algorithms", ICASSP '93-V, pp. 301-304.

[28] W. W. Zin, "Message Embedding In PNG File Using LSBSteganographic Technique", International Journal of Science and Research, Vol. 2 No..1, 2013

[29] V. Tyagi, A. Kumar, R. Patel, S. Tyagi and S. S. Gangwar, "IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY", Journal of Global Research in Computer Science, Vol. 3, I. 3, 2012

[30] M. Mohamed, F. Al-Afari, and M. Bamatraf, "Data Hiding by LSB Substitution Using GeneticOptimal Key-Permutation", International Arab Journal of e-Technology, Vol. 2, No. 1, 2011

[31] S. Gupta, A. Goyal, and B. Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I.J.Modern Education and Computer Science,Vol. 6, pp. 27-34, 2012