

# Steganographic Software: Analysis and Implementation

AKRAM M. ZEKI<sup>1</sup>, ADAMU A. IBRAHIM<sup>2</sup> AND AZIZAH A. MANAF<sup>3</sup>

<sup>1,2</sup>Faculty of Information & Communication Technology,  
International Islamic University Malaysia, Malaysia, MALAYSIA

<sup>3</sup>Advanced Informatics School (AIS),  
University Technology Malaysia, MALAYSIA

<sup>1</sup>[akramzeki@iium.edu.my](mailto:akramzeki@iium.edu.my) <sup>2</sup>[adamuabubakar9@gmail.com](mailto:adamuabubakar9@gmail.com) <sup>3</sup>[azizah07@ic.utm.my](mailto:azizah07@ic.utm.my)

*Abstract*—Steganography is the method of hiding data in such a way that no one, except the sender and the intended recipient, expects the existence of the hidden data. Thus the goal here is always to conceal the very existence of the secret data embedded in an innocent data in such a way that it will be undetectable, robust and the innocent data should be able to accommodate high capacity of the secret data. Unfortunately, these goals were not commonly seen in most of the techniques. This paper studied different Steganographic techniques and undertakes an experiment using five Steganographic software in order to explore their capabilities. Benchmarking tool for identifying different performance aspects of the Steganographic techniques and Steganographic software like visual quality, performance indices, memory requirement and the evaluation of the maximum capacity for each software under this study. Experimental results show that all the software under this study performs above optimal level, although there are some differences of features and capabilities observed.

*Keywords*—Steganography, Steganographic Software, Information Hiding, Steganographic tools, PSNR.

## I. INTRODUCTION

**I**NFORMATION is vital to human effort; indeed digital information offers wonderful opportunities and

improvements to human life, especially with the advent of internet. The internet has become the most important source of information, which offers ubiquitous channels to deliver and exchange information.

The term Steganography which was earlier described as Steganographia first appears in a manuscript by Johannes Trithmius that started in 1499 [1]. The goal here is to hide data inside other harmless data in way that does not allow any suspicious present of the hidden data so that it can be used as a medium for transmission of secret information. Embedding secret data, into harmless data requires the presents of the two files. The first is the innocent-looking file that will hold the hidden information called the host file. The second file is the secret message. A message may be plaintext, cipher text, or any bit stream. When combined, the host file and the embedded message make a Stegofile.

Over the years, many algorithms were proposed for steganographic technique, the common approaches include: Least significant bit insertion, Masking and filtering, Transformations. [2] Each of these techniques can be applied, with varying degrees of success. The strength of each technique relies on robustness, image quality (imperceptibility) and capacity, by definition it means the ability of information to be hidden in a carrier medium without any suspicious clue of the present of any embedded information. These have been found that when the robustness of the watermarking method improves, the imperceptibility decreases, and the capacity increases. In addition, there is also a tradeoff between these requirements and this should be taken into account whenever the steganographic method is proposed. One of the important considerations of digital steganography is that the presence of the hidden message be undetectable. [3] This means that files with and without secret message should appear identical to all possible statistical tests which can be carried out. Another important consideration is robustness. A robust technique means the ability of the secret message embedded in a carrier file to retain its states, without been degraded by any means and

maintains its quality. The final important consideration is the capacity of the communication channel. In this aspect, the challenge is to embed as much information as possible in the carrier file, while still maintaining the state of the carrier file without any distortion. Example like in image file, its quality should be retained while embedding secret file so that it does not affect the quality of the underlying secret data. The secret file is truly imperceptible if the carrier data cannot be distinguished from its states before the embedding of the secret information. However, since users normally do not have access to the carrier file before the embedding process, they cannot perform any comparison between the file that contain the secret information and the file that secret information is not embedded on, that is, if only the steganographic technique is efficient enough. Therefore, it is sufficient that the modifications in the carrier data go unnoticed, as long as the data is not compared with the original data

Robustness refers to the ability of the inserted information to withstand modifications (intentional or unintentional). The secret information should be difficult to remove or alter without the degradation of the host image [4], [5]. However, it is important to note that the level of robustness required varies with respect to the application at hand. To verify the robustness of the watermarking technique, different parameters has been used to assess robustness such as the Bit Correct Ratio (BCR) which was used by [6] or the Bit Error Ratio (BER) used by [7] and [8] The similarity theory has been used in another study [9] and probability has been employed by [10]. Although these methods refer to the same concept and give almost the same result, the normalized cross correlation (NCC) used in the many study considered 13 the most famous and mostly used parameter for testing the robustness of steganography [11]

Capacity refers to the amount of information being able to be inserted into a particular image. Low SNR is a phenomenon of steganographic channels, which severely limits the capacity. For steganographic file, many bits like hundreds or even thousands may be needed [12]. The challenge is to embed as much information as possible while staying compatible with the image noise model. In general, increasing the capacity will make the secret file more obtrusive in viewing. In addition, the steganographic system is more robust when the secret file signal power rises [13]. Under the present day scenario, the rough estimates of the low, medium, high and very high payloads, particularly for images, are 0-2%, 2-10%, 10-20%, >20% respectively [14]

Steganographic technique can be attacked either through scanning of an entire file system, individual directories, or individual files on suspected media for the presence of known signatures of particular steganography applications, or by identifying files that have information appended beyond the file's end-of-file or identifying files that have information embedded using Least Significant Bit (LSB) image encoding with the LSB Analysis feature and extract and rearrange the LSBs for analysis in a hex editor view to determine if information has been hidden within the file. However, almost

all steganographic software comes with their strengths and weaknesses, and they are mostly based on different techniques and algorithms. Some are open source, while others were obtained by licenses.

Although many information hiding techniques have been proposed by various authors, the specific requirements of each Information Hiding technique vary with the application. This study aims at providing a test for a proof of performance to explore the best and current Steganographic software available, and the most outstanding Steganographic technique.

The remaining part of this paper is organized as follows; section 2 discuss the related work, section 3 discuss the research experiment and section 4 discuss the software evaluation, section 5 discuss the result and finally section 6 discuss the conclusion of the work.

## II. RELATED WORK

Modern steganographic techniques have far more powerful tools that attract many giants' commercial companies whose wish are to safeguard their information from piracy and imitation. As a result, most efficient steganographic techniques will provide proficient means of information protection.

There are many on-going researches aimed at unveiling the most efficient steganographic techniques, among which are, the work of L. Y. Por 2008, which presents an overview of text steganography by Hiding information in manipulation of whitespaces between words and paragraph which offers dynamic generated stego-text and generate a cover-text dynamically by offering six options for user according to their length of the secret message [2], [3]. Yun, C. 2010, Present a method for checking the acceptability of paraphrases in context by using the Google n-gram data and a CCG parser to certify the paraphrasing grammaticality and fluency, which automatically generated paraphrases as a new and useful source of transformations for Linguistic Steganography which is in a specific dedicate language and domain independent, requiring only a paraphrase dictionary and a Google n-gram corpus. [4]

L.Y. Por 2008b also presents an overview of steganography on GIF image format in order to explore the potential of GIF in information hiding research. He explore the enhancement of the Least Significant Bits (LSB) insertion techniques from the most basic and conventional 1 bit to the LSB colour cycle method and integrate three algorithms in one steganography system it also focused in assimilation of diversified methods into a whole gamut of steganography systems [5]. Nair, A.S present a steganographic technique that sends secret data in the length of the network packets the length of UDP datagram is modified to embed the secret data on a UDP based chat application and obtained the length pattern, which follows the normal network flow even after embedding the secret data [6]. Cui-ling J. 2011 present a steganographic technique based on JPEG digital images, in their approach, instead of dividing cover-image into 8x8 blocks, non-overlapping

blocks of  $16 \times 16$  pixels is used and a quantization table is constructed, the DCT coefficients are quantized and embedded the secret messages [7] Banoci, V. 2011 also present a steganographic technique using transform domain of Discrete Wavelet transform (DWT) by modifying of transform coefficients in an appropriate manner which do not require original image for successful extraction of the secret information [8].

All the related work on the steganographic techniques reviewed in this research was seen to be experimentally tested and the proofs of the performances were at the testing level. What we did compare to the above related works is testing some techniques at the implementation level in order to proof the performances.

### III. EXPERIMENT

This study starts with selecting the Steganographic software based on the random sampling within the most commonly accessible steganographic software, out of these samples; five were chosen in order to study their features and capabilities. The next step is studying the benchmarking parameters that will be used for testing the software's performances in order to determine their differences. Then followed by undertaking an experiment with each software. The experiment involves embedding and extracting of information on the carrier file and checking for their performance using benchmarking tools and applying some attacks on the carrier file to see if it can be detected which will then be compared for all the five software used in the study.

Six standard Host Images have been selected in this study (Four gray scale images, with size of  $(256 \times 256)$  Pixels 192 KB, see Figure 1) and (two colors images, with size of  $(512 \times 512)$  Pixels 768 KB, see Figure 2). In addition one image to be hidden within the host images called logo (with size of  $(84 \times 84)$  Pixels 20.7 KB see Figure 3) was selected here. All these images are BMP image format.

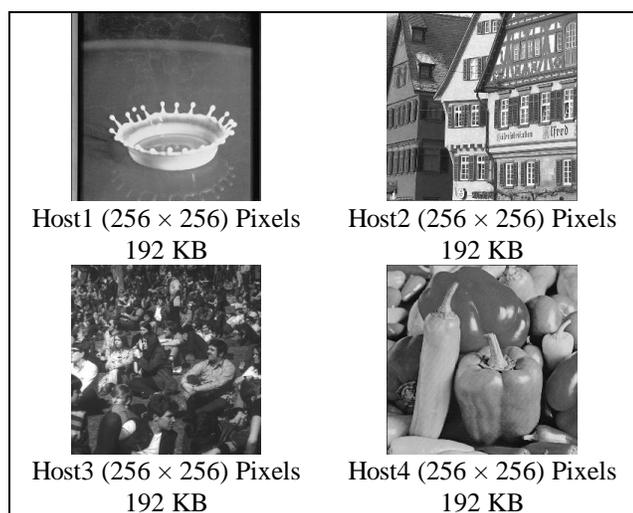


Fig. 1 Gray scale Standard Images for Steganography.

The images above are the grayscale image files that were used to embed information inside them; over here we use the image file of figure 3 to embed in the entire grayscale files and the color image files of figure 2. The difference between grayscale and images is the sizes.

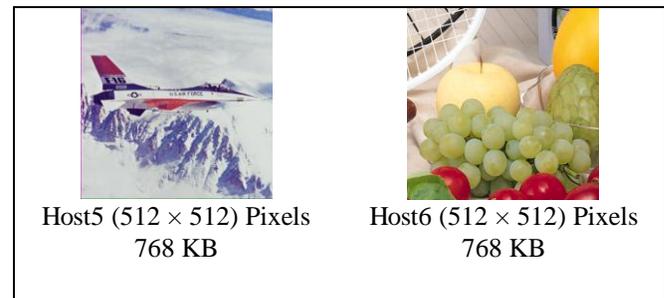


Fig. 2 Color Standard Images for Steganography

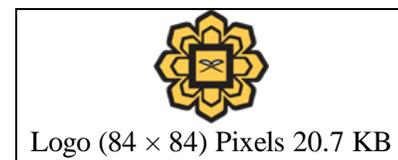


Fig. 3 Image that will be hidden.

Steganographic algorithm is reliable when it embeds the secret message with little distortion so that it does not affect the quality of the underlying host file. The secret message should be truly undetectable, so that the host file cannot be distinguished from the Stego file. After embedding, distortion normally occurs which in turns affects the Stego file. To ensure that the distortion caused by embedding process is acceptable to Human Visual System (HVS), quality metrics are used to measure the difference between the host file and Stego file. Examples of such metrics are Mean Square Error (MSE), PSNR. The Mean Squared Error (MSE) is the averaged term-by-term squared difference between the input signal (the original image,  $P$ ) and the output signal (the secret message,  $P'$ ), as shown in below Equation.

$$MSE = \frac{1}{N} \sum (P'_i - p_i)^2 \quad (1)$$

The PSNR is given in below Equation in which  $P_{peak}$  is the peak value of the input signal.

$$PSNR(db) = 10 \log_{10} \frac{P_{peak}^2}{MSE} \quad (2)$$

Usually 255 for 8 bit Gray scale images [9], [10], the larger the PSNR, the better the image quality will be. Some researchers considered the acceptable quality of Stego image, when the PSNR was greater than 30db [11], [12].

## IV. STEGANOGRAPHIC SOFTWARE EVALUATION

Almost all Steganographic software comes with their strengths and weaknesses, and they are mostly based on different techniques and algorithms. It's a fact that each Steganographic software has been designed by different company, and developed by different programming language. Some are open source while some are not, and other comes as part of security suite software.

This study aimed at comparing the features and capabilities of most popular and current Steganographic software available. Five Steganographic software have been selected. Six host images, four gray scale images and two color images are the images considered for this research as indicated in Figure 2 and 3. The host images are the standard images for Steganography and they were downloaded from the internet. They can be found in many websites. The software selected for the comparisons are: Invisible Secrets 4, Hermetic Stego 8.04, Puffer 4.04, Xiao Steganography 2.6.1, and S-Tools

Invisible Secrets 4 is a powerful security suite that can hide and encrypt files, also can destroy internet traces, shred files, make secure IP-to-IP password transfer and even lock any application on the computer. It is an easy to use with a powerful wizard interface. It was first released in 1999; the latest version is "Invisible Secrets 4" that was released in 2009 by NeoByte Solutions. It accepts five hosts file formats Steganography applications, which are: JPG, PNG, BMP, HTML and WAV.

Puffer version 4.04 was released as a revised version of Puffer 4.03 in 2009. It is a general purpose encryption and Steganographic software that is used to protect most sensitive data from unauthorized viewing to securely exchange

message or email with other Puffer users. It hides data among the pixels of image, and distributes self-decrypting archives to non-Puffer users. Extensive wiping options are also available to permanently erase sensitive data. Puffer runs on all 32-bit versions of Windows from 98 through Vista. Puffer 4.04 has displayed the ability to hide encrypted archives among the pixels of 24-bit color image, specifically PNG and BMP files.

Xiao Steganography 2.6.1 is developed by nakasoft (www.nakasoft.net) in Venezuela. It is easy to use and powerful wizard interfaced. It was released in 2005; it offers an impressive and unique art of hidden writing. It accepts many different types of file. The security level use RC2, RC4, DES, Triple DES, Triple Des 112 and Hashing MD2, MD4, MD5, SHA Algorithms through using password protected.

Hermetic Stego 8.04, is part of Hermetic applications under Hermetic system which was released on 2009. Hermetic Stego is able to hide any type of file within BMP images, with an encryption key, so that the presence of the hidden file is undetectable, if a Stego key has been used when hiding the data then that data can be extracted only by someone who knows that Stego key. The Stego key is used not only to facilitate random selection of bytes for hiding data file bits but also is used to encrypt the data file.

S-tools, was developed by Andy brown in 1996. S-Tools is a Steganography tool that hides files in BMP, GIF, and WAV files. It can hide multiple files in one sound/picture and the data is compressed before being encrypted and then hidden. Multi-threaded operation means that the user can have many hide/reveal operations going simultaneously without fear of them interfering with other work. The user can even close the original picture/sound with no ill effects to ongoing threads.

Table 1. The Steganographic software features used in this study.

Steganographic Software	Software Size	Software Description	Software Creator	Software Sources
Invisible Secrets 4	2.7 MB	Security suite software that can hide files, encrypt files, destroy Internet traces, shred files, make secure IP to IP password transfer and even lock any application on the computer	NeoByte Solutions	1. <a href="http://www.invisiblesecrets.com/download.html">http://www.invisiblesecrets.com/download.html</a>
Hermetic Stego 8.04	2.30MB	Uses encryption and hiding technique to hide files of any type and of any size in BMP images, with or without the use of a user-specified Stego key	Hermetic system	1. <a href="http://www.hermetic.ch/hst/hst.htm">http://www.hermetic.ch/hst/hst.htm</a>
Puffer 4.04	1.90MB	It a security is general purpose encryption and Steganographic software; with Extensive wiping options are also available to permanently erase sensitive data.	Briggs Softwors	1. <a href="http://www.soft32.com/download_7842.htm">http://www.soft32.com/download_7842.htm</a>
Xiao Steganography2 .6.1	2.14MB	It is security software that implements cryptography/Steganography. It offers unique art of encrypting and hidden files. It can Includes attach any file, doesn't matter the type of file (limited by the size of host image)	Nakasoft	1. <a href="http://download.cnet.com/XiaoSteganography/30002092_410541494.html">http://download.cnet.com/XiaoSteganography/30002092_410541494.html</a>
S-Tools	561 KB	It is a Steganography that hide files in BMP, GIF, and WAV files. And also uses some encryption technique as an added layer of security.	Andy brown	1. <a href="http://www.jjtc.com/Security/Stegtools.htm">http://www.jjtc.com/Security/Stegtools.htm</a>

S-Tools use the spatial domain technique and works by spreading the bit-pattern of the file that will be hidden across the least significant bit. S-Tools use four encryption options

(IDEA, DES, Triple DES and MDC) that give an additional security level to its operation. After embedding the message, normally distortion occurred which in turns affect the Stego.

The features of the software under this study were represented in table 2; they all come with Graphical User Interface (GUI), some come in collection of security applications while others are specifically for Steganographic use only. The capabilities of the software (The Image format, Capacity, Cryptographic algorithm and Steganographic techniques). Notice that the capacity refers to the amount of

information being able to be inserted into a particular image. In general, increasing the capacity will make the hidden image more obtrusive in viewing.

Measuring the embedding capacity can be done directly by dividing the size of the embedded information on the size the host image

Table 2. Capabilities of steganographic software under this study

Steganographic Software	Host Image Formats	Software Capacity	Memory Usage	Encryption Support	Steganographic Algorithm
Invisible Secrets 4	BMP, JPG, PNG	12.80%	10.104 KB	AES-Rijndael, Twofish, RC4, Cast128, GOST, Diamond 2, Sapphire II, and Blowfish	least significant bits (LSB) algorithm
Puffer 4.04	BMP, JPG, PNG, GIF	38.40%	4.512 KB	AES encryption algorithm	least significant 3 bits (Intermediate bit )
Hermetic stego 8.04	BMP	12.20%	8.22 KB	DES encryption algorithm ME6 encryption	LSB technique,
Xiao Steganography2.6.1	BMP	12.50%	6.256 KB	RC2, RC4, DES, Triple DES, Triple Des 112 and Hashing MD2, MD4, MD5, SHA	least significant bit (LSB) substitution
S-Tools	BMP, GIF, WAV	12.80%	1.224 KB	IDEA, DES, Triple DES and MDC	least significant bit (LSB)

Notice that the capacity refers to the amount of information being able to be inserted into a particular image. In general, increasing the capacity will make the hidden image more obtrusive in viewing.

Measuring the embedding capacity can be done directly by dividing the size of the embedded information on the size the host image.

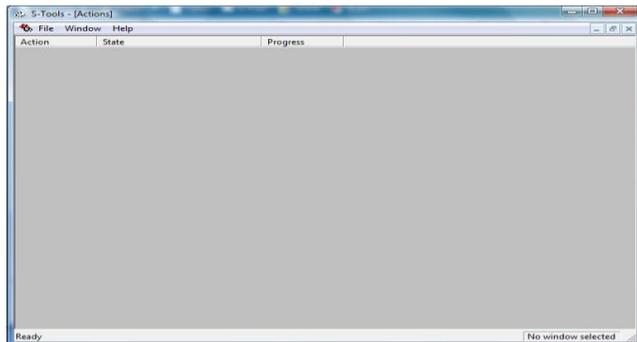


Fig. 4 S-Tools user interface



Fig. 5 Invisible Secrets 4

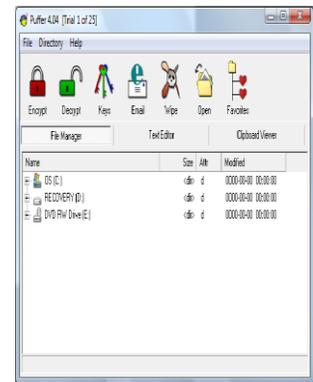


Fig. 6 Puffer 4.04

V. RESULTS AND ANALYSIS

After embedding, the qualities of images were determined. In most applications, hiding algorithm must embed the secret file/files so that it does not affect the quality of the underlying host file. The secret file/files should be truly undetectable, so that the host file cannot be distinguished from the stego image. It's a fact that an ordinary person that sees the stego image may not have previous knowledge of the image; as a result he cannot perform comparison. Therefore, it is sufficient that the modifications in the stego image go unnoticed, as long as the stego image is not compared with the host image.

The image quality measure after embedding process, high image quality reflects the success of Steganographic system. PSNR has been used for measuring the quality of image. All host images were converted to BMP format before embedding process for comparison purposes. Table 3 shows the PSNR



Fig. 7 XiaoSteganography2.6.1

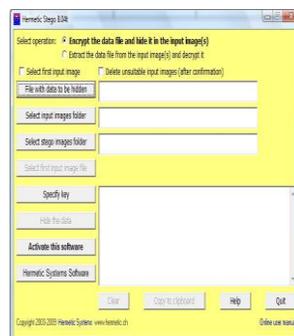


Fig. 8 Hermetic stego 8.04

Table 3 PSNR of the Software

HOST IMAGES	Invisible Secrets 4	Hermetic Stego 8.04	Puffer 4.04	Xiao Stegano-graphy2.6.1	S-Tools
Host1	51.14	50.81	43.21	51.7689	56.39
Host2	51.14	50.07	49.15	57.7948	62.43
Host3	51.14	50.81	43.15	51.7704	56.40
Host4	51.14	50.85	43.06	51.7911	56.38
Host5	51.14	50.81	43.17	51.7508	56.41
Host6	51.14	50.07	49.15	57.7956	62.43

Values after embedding the logo image within the host images using the selected software.

This study uses a single watermark file to be embedded within all host images using the five different software. Invisible secret 4 reveals that the PSNR were all the same. The above results, indicates that S-Tools shows better

performance, while Puffer 4.04 is the least. While though, all the software's PSNR were above 40 dB, which is above the benchmark for the most high quality Stego image, it still reveals that Hermetic Stego 8.04, Invisible secrets 4, and Xiao Steganography 2.6.1 performance were relatively the same

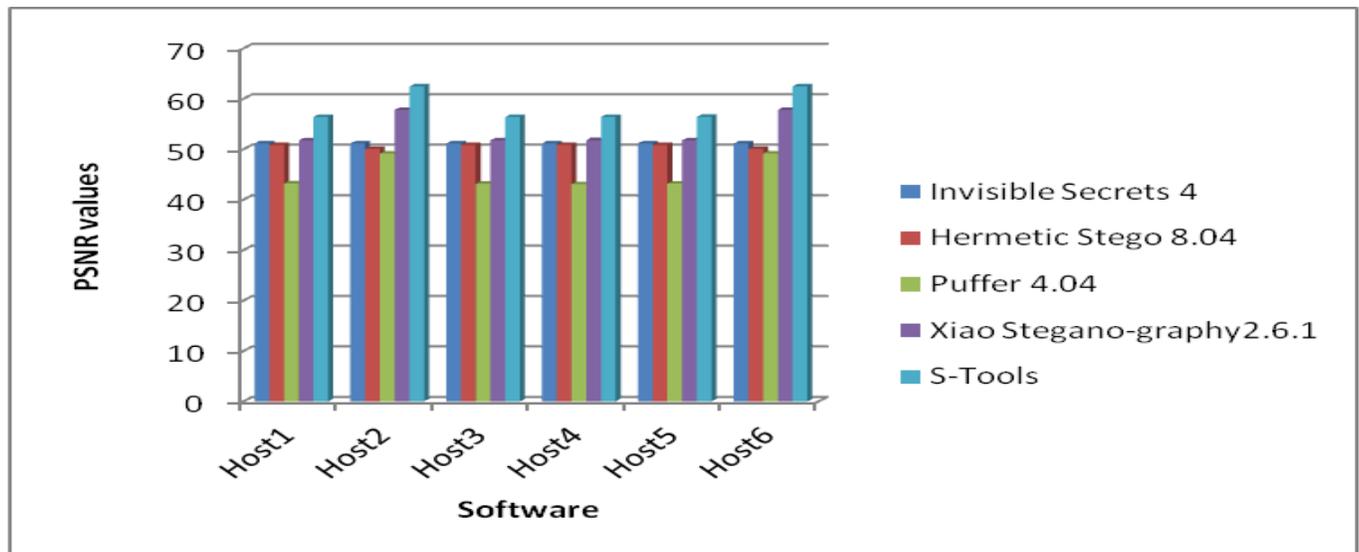


Fig. 9 PSNR of the software

The results show that all the software possesses the ability to hide data without noticing changes in their properties, more especially the image size which logically is the second character to be considered to ensure efficiency of hiding system apart from visual inspection of the Stego image. The entire extracted images were clear without any distortion. The techniques uses by all the software under this study were found to be the spatial domain embedding techniques, this technique were faced with some drawbacks, among which are the embedding capacity: that is the Capacity of information storage is limited and algorithms are generally not robust to geometric and compression attacks. Vulnerable to slight changes: that is the stego images are vulnerable to even a slight image distortion, such as simple conversion from BMP or GIF to a lossy compression format like JPEG can destroy hidden image. Image quality or the carrier file quality: Image degradation and visual artifacts are more pronounce in spatial domain watermarking

because of random changes especially in LSB. The cost of computation: embedding in spatial domain is computationally inefficient because the original image is needed for extraction of the secret data

These problems can be resolved through the use of transform domain embedding. By embedding using Transform is simply means mapping from one set of coordinates to another. To obtain better imperceptibility as well as robustness, the addition of the secrete message/watermark is done in a transformed domain [31], [32]. Scientist exploited the benefits of frequency domain transformation like Discrete Cosine Transform(DCT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT), Fast Hartley transform (FHT), Hadamard Transform, Mellin transform and Discrete Wavelet Transform (DWT) to build a robust watermarking algorithm. The transformation can be applied to the image as a whole or to its subparts. The watermark casting is done by modifying some coefficients, which are

selected according to a watermarking rule. In both cases the modifications should not distort the image, that is, those modifications should not be visible. Transform-based techniques are very robust against attacks involving image compression and filtering because the watermark is actually spread throughout the image. Frequency-based watermarking also offers increased robustness to scaling and rotations or cropping, depending on the invariant properties of a particular domain another reason for steganography in frequency domain is that the characteristics of Human Visual System HVS is better captured by the spectral coefficient and less sensitive to high frequency [33].

## VI. CONCLUSION

This research presented a background of Steganography and a comparative study of some Steganographic software. Steganography as information security system can have some useful applications, like other seemingly related system (cryptography). The success of this study is to identify the reliable and best software available in the market for Steganography. Some of the software available in the market were selected based on the recent deployment that is five recently deployed software, these software were tested using the same input on all of them. The tools used in our experiment are images. Specific image was embedded within all host images for each of the five software selected.

The results of the experiment reveal that all the five software were relatively performing at the same level, though some software performs better than others. The image quality measure after embedding usually reflects the success of Steganographic system. The tool for measuring the quality of image after embedding is the PSNR. The values of PSNR are obtained using the software under this study were all above the bench mark for the high quality image. However the steganographic techniques used in the developing of the software were all seen to be meant for spatial domain embedding and these techniques alongside transform domain technique were studied.

Embedding in the spatial domain provide easy insertion and simple approach by directly embedding information in an image file which is done by changing the pixel position, while embedding in transform domain is based on transformation of the host signal to desire domain before embedding take place. Usually secret information is spread across the host signal's frequency spectrum as much as possible. The weakness of using spatial domain is that carrier file's, quality (be it image or not image file) may be degraded after embedding, while using transform domain it's proving that no visual degradation after embedding can be seen especially when the position to embed is well defined.

## REFERENCES

- [1] M.K. Arnold, M. Schmucker, and S.D. Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection", Artech House, Norwood, Massachusetts.
- [2] K.S. Ntalianis, "A Short-Message Robust Steganographic Method for Effective Information Recovery Under Transmission Losses of Cellular Networks", *Proceedings of the 9th WSEAS International Conference on Systems*, Greece, 2005, pp. 955-957.
- [3] J. J. Liaw, L. H. Chang, Y. S. Liao, "An Improvement of Robust and Blind Data Hiding Based on Self Reference in Spatial Domain", *Proceedings of the 2007 WSEAS International Conference on Computer Engineering and Applications*, Gold Coast, Australia, 2007, pp. 259-263.
- [4] G. Voyatzis, and I. Pitas, "Protecting Digital-Image Copyrights: A Framework", *IEEE Trans on Computer Graphics and Application*. 19(1): 18-24. 1999.
- [5] W. Y. Chen "A Comparative Study of Information Hiding Schemes Using Amplitude, Frequency and Phase Embedding". Ph.D. Thesis 2003. National Cheng Kung University, Taiwan.
- [6] R.O. Duda, P.E. Hart, and D.G. Stork, "Pattern Classification". (2nd Ed.) New York: John Wiley & Sons, Inc. 2001
- [7] J.A. Briffa, and M. Das, "Channel models for high-capacity information hiding in images". *The International Society for Optical Engineering Journal*. 135-144. 2002.
- [8] F.T. Syed, A.A. Khan, and M.M. Anwar. "Support Vector Machine based Intelligent Watermark Decoding for Anticipated Attack", *Transactions on Engineering, Computing and Technology*. October. 15: 2006.
- [9] S.A. M. Gilani, and A.N. Skodras, "Multiple Channel Watermarking of Color Images", Technical Report No. Tr2002/02/03. Academic Research Computer Technology Institute. Greyscale Standard Images. 2002.
- [10] L.M. Matt, and A.B. Jeffrey, "Computing the Probability of False Watermark Detection", *Third International Workshop on Information Hiding*. Dresden, Germany, 1999.
- [11] S.P. Maity, and M.K. Kundu, "Robust and Blind Spatial Watermarking In Digital Image", *Proceedings of 3rd Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP '2002)*. 16-18th December. Ahmedabad, India: 388-393.
- [12] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "Capacity of the watermarking channel: How many bits can be hidden within a digital image". *Security and Watermarking of Multimedia Contents*, *Proceedings of SPIE*, Wong, Delp. San Jose, CA, 3657: 437-448. 1999.
- [13] P.C. Chen, "On the Study of Watermarking Application in WWW – Modelling, Performance Analysis, and Applications of Digital Image Watermarking Systems". Ph.D. Thesis 1999, Monash University.
- [14] A. Viterbi, "CDMA: principles of spread spectrum communication", Redwood City, CA, USA: Addison Wesley Longman Publishing Co. Inc 1995.
- [15] L. Y. POR, B. Delina Information Hiding: A New Approach in Text Steganography 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008
- [16] L. Y. Por1, T. F. Ang2, B. Delina3 WhiteSteg: A New Scheme in Information Hiding Using Text Steganography WSEAS TRANSACTIONS on COMPUTERS ISSN: 1109-2750 Issue 6, Volume 7, June 2008
- [17] Ching-Yun Chang and Stephen Clark Linguistic Steganography Using Automatically Generated Paraphrases *Proceedings of the Annual Meeting of the North American Association for Computational Linguistics (NAACL-HLT-10)*, pp. 591-599, Los Angeles, 2010
- [18] L.Y. Por1, W.K. Lai2, Z. Alireza3, B. Delina4 StegCure: An Amalgamation of Different Steganographic Methods in GIF Image 12th WSEAS International Conference on COMPUTERS, Heraklion, Greece, July 23-25, 2008 ISSN: 1790-5109
- [19] A. S., Nasir, A., Kumar, A Sur, S. Nandi., Length Based Network Steganography using UDP protocol. 3<sup>rd</sup> International Conference on Communication Software and Networks. (ICCSN), 2011 IEEE 10.1109/726 – 730.
- [20] Cui-ling Jiang; Yi-lin Pang; YuZhu, Y.; A steganographic method based on the JPEG digital images 3<sup>rd</sup> International Conference on Computer Research and Development (ICCRD), 2011 Volume:3 10.1109/ICCRD.2011.5764240 2011, Page(s): 35 – 38.
- [21] Banoci, V.; Bugar, G.; Levicky, D. A novel method of image steganography in DWT domain; 21<sup>st</sup> International Conference on Radioelektronika (RADIOELEKTRONIKA), 2011 10.1109/RADIOELEK.2011.5936455 2011, Page(s): 1 – 4

- [22] Joachim, J., Eggers, J. & Bernd, G. (2000). Robustness of a blind image watermarking scheme. ICIP 2000, Special Session on WM. Sep. 10–13. Canada.
- [23] Stefan, W., Elisa, D. & Gelasca, T. (2002). Perceptual quality assessment for video watermarking. Proceedings of International Conference on Information Technology: Coding and Computing (ITCC). April 8-10. Las Vegas, NV
- [24] Wu, N. (2004). A Study on Data Hiding for Gray-Level and Binary Images. Master Thesis. Chaoyang University of Technology, Taiwan.
- [25] Bennour J. Dugelay J. L. & Matta, F. (2007). Watermarking Attack: BOWS contest. Proceedings of SPIE.
- [26] N. Agarwal and A. K. Goyal, “Robust Watermarking in Transform Domain using Edge Detection Technique”, *IEEE Inter. Conf on Computational Intelligence and Multimedia Applications*, pp.59-63,2007.
- [27] E. E. Abdallah, A. B. Hamza, and P. Bhattacharya, “ A robust block based image watermarking scheme using Fast Hadamard transform and singular value decomposition”, *18th IEEE International Conference on Pattern Recognition (ICPR'06)*, vol. 3, pp 673 – 676 , 2006.
- [28] A. Piva, M. Barni, F. Bartolini, V. Cappellini, “DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image”, *Proceedings of IEEE Inter. Conf. on Image Processing 1997 (ICIP 97)*, Santa Barbara, CA, USA, vol. 1, pp. 520 - 523, October 1997.