Evaluation of Multi Level System of Steganography

Tunde J. Ogundele*‡, Adebayo O. Adetunmbi**

Department of Computer Science, Federal University of Technology, PMB 704, Akure, Nigeria.

e-mail: * tjogundele@futa.edu.ng, ** aoadetunmbi@futa.edu.ng

‡ Corresponding Author; Address: Tel: +234 806 711 1876, e-mail: tjogundele@futa.edu.ng

Abstract- This paper proposes and evaluates a multi-level system of steganography (MLSS) which is a combination of steganography, cryptography and compression. Data encryption standard is the encryption algorithm used while the compression algorithm is Lempel-Ziv. Our approach scans through each of the cover image pixels, encodes the message bits with the green object of the pixel component and replaces the blue object with it. In evaluating the performance of the proposed work, several tests were carried out and recordings taken. The compression algorithm yields 91% average compression rate on the dataset. The efficiency of the MLSS was determined by testing it against xsteg stegodetect steganalysis software and comparing its peak signal to noise ratio (PNSR) with that of two existing steganography applications - P2P and Quickstego. The average computed PNSR for MLSS, Quickstego and P2P are 67.78, 61.18 and 54.01 respectively. The proposed scheme yielded a stego image with large hidden capacity, improved hidden message security, and high PNSR value.

Keywords- Steganography, compression, encryption, peak signal to noise ratio

1. Introduction

Steganographic technologies are very important part of the Internet security and privacy on open systems [1]. Steganographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment [2]. There are quite number of researches in the field of steganography and many applications of steganography have been developed. Steganography is the art and science of communicating in a way which hides the existence of the communication [3,4]. In this sense, message or information sent will not attract suspicion to themselves, to messengers or to recipients [3,5,6].

In this paper, an evaluation of our approach used in [3] is carried out and a comparative analysis of its application against some of the existing steganography applications is documented. The efficiency of MLSS was determined by comparing its peak signal to noise ratio with that of p2p and quickstego application on Hydrangea, Jellyfish and Lena images. The proposed scheme developed in [3] encrypts and then compresses the message intended for concealment. The rest of the paper is organized as follows: section 2 discusses the review of related works and applications, section 3 discusses the proposed scheme. In section 4, the concept of peak signal to noise ratio is discussed while results, evaluation and comparisons are done in section 5.

2. Review of Related Works

In an attempt to address the security of information in transit using steganography, the following are some of the work that has been done.

Amanpreet et al., used an approached that is based on first component alteration [4]. They replace the blue component of each pixel with secret data bits in their embedding technique.

Gandharba, and Saroj in [7] developed a technique for secret communication using a new

block cipher, they encrypt the secret message by cryptography algorithm block cipher with dynamic steganography. In their approach, two cipher text bits are embedded in each pixel of the gray scaled image. The embedding locations are two of 6^{th}, 7^{th} and 8^{th} pixel bit location depending upon the cipher text bits which are decided at the run time of the algorithm.

Rupinder et al., in [8] proposed a model that allows image to acts as a shared key between the sender and receiver. Every character in the text is converted into its integer value which is mapped to the single pixel value of the image.

Steganography applications known as P2P and Quick stego are developed by [9] and [10] respectively. P2P application is implemented using C# and .Net framework 3.5, the scope is to hide information that include any type of text or image file and the path where the user wants to save Image and extruded file. Quickstego scope enables users to hide text in pictures so that only other users of the application can retrieve and read the hidden secret messages.

3. Proposed Scheme

The system requires a user to supply a secret message, key, and the cover image file. The secret message is encrypted with the key and compressed which gives a compressed file with reduced size. The encryption scheme used is data encryption standard (DES) while the compression scheme is Lempel-ziv. The proposed design is shown in Figure 1.

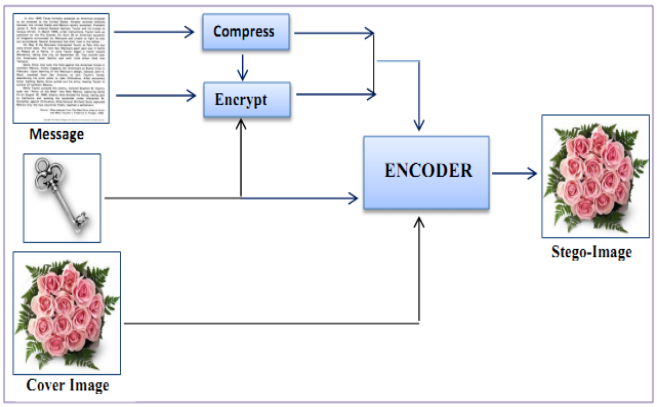

Fig. 1. Proposed system design [3].

At the encoding section, the system generates a constant C gotten from the system date as shown in Eq. (1), where d is day in system datetime and m is month in system date-time object. The key and the message are converted to byte array, each byte is encoded with the constant. The essence of this is to increase the security of the secret message and to also serve as our terminator which distinguishes the key from the message during embedding phase.

$$C = d + m \tag{1}$$

An image is an array of numbers that represent light intensities at various points, or pixels. In this scheme, 24-bit per pixel image is used. The process of message insertion starts with inserting the secret key bytes in the image, constant bit (which serves as the terminator) after which the message bytes are inserted. To insert the message bytes, our approach scans through each pixels (each pixel has R, G, and B components) of the image, and the blue object of each pixel component selected is replaced with the each key byte. After all the key bytes have been inserted, we insert constant byte (the terminator) and secret message byte insertion follows.

The process of inserting secret message is quite similar to that of secret key insertion but different. Each of the blue object of the pixel is not only replaced with the secret message but the green object (gb) of the pixel is encoded with the message byte (mb) as indicated in Eq. (2) and resulting encoded byte (eb) is used to replace the blue object of that same pixel component. This process is repeated until all the message bytes have been inserted.

$$eb = gb \oplus mb \tag{2}$$

4. The Concept of Peak Signal to Noise Ratio

In order to estimate the quality reconstructed stego image, we use peak signal to noise ratio (PNSR). PNSR is defined as an expression that represent the ratio between the maximum possible value of a signal and the power of error (noise) on its representation [15]. The signal is the original data while the noise is the error caused by compression [1,12]. Generally, when a PNSR value of a signal is high, such reconstructed signal has lower noise [15].

If mean square error (MSE) which is a measure of the average square error is given as:

$$MSE = \frac{1}{m.n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (3)$$

In a case where colour image usually with three (RGB) values per pixel is used as cover, the MSE is the sum over all squared value differences divided by image size and by three [13].

PNSR is defined as:

$$PNSR = 10.\log_{10}\frac{MAX_1^2}{MSE} \qquad (4)$$

$$PNSR = 20.\log_{10}\frac{MAX_I}{\sqrt{MSE}} \qquad (5)$$

Where MAX_I represent the maximum pixel value of the image.

5. Result, Evaluation and Comparisons

To evaluate the performance of the proposed work, the application developed from the proposed design (multi-level) is applied on Hydrangea, jellyfish and Lena's images as test images that are shown in figure 2. We show the effect of the compression algorithm on the text file and corresponding effects on these test images as indicated in graph shown in figure 3. The strength of the security measure of our model was tested against xsteg stego-detect steganalysis software and the result was negative. Xsteg is a graphical frontend to stegdetect. It is a utility for automated detection of steganographic content in JPEG images [14]. To measure the stego image quality of the proposed approach, we used Peak Signal-to-Noise Ratio (PSNR) and the MSE (Mean Square Error) for the stego images as indicated in table 1.

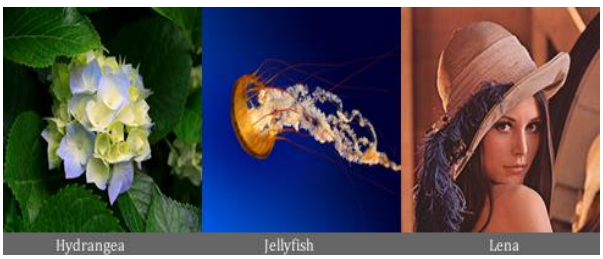

Fig. 2. Images showing Hydrangea, Jellyfish and Lena

Table 1 shows the PNSR values comparison between the applications developed from the MLSS approach and existing steganography applications (P2P and QuickStego). The results show that application developed using our method has higher PNSR than both P2P and quickstego. Hence, proposed method provides a better stego image quality.

In addition, when the size of the plaintext file reaches 113KB as shown in the table, the quickstego application can no longer embed the text into the image as it reports large text (LT) errors. This shows that the application has limited file size. At this file size the quality of the stego image produced by P2P application has dropped as indicated by its PNSR values in the table and the difference of the stego image and the original is noticeable to the human eye.

6. Conclusion

Current electronic steganographic methods are not as necessarily secure due to the size of the data they hide and the approach they used in embedding information in a cover image. Taking the cover into account, it is likely to increase the security of the message by encoding the area of the image's pixel where the information is hidden.

In this paper, we have shown that the system is better when the secret message is compressed as it allows more data to be embedded. Also, the quality of the reconstructed (stego) image is better compared to that of p2p and quickstego applications. So in conclusion, as emphasis is placed on the area of security, privacy protection, it is believed that this research will do exactly that by improving on the security and the hiding capacity of the existing technologies.

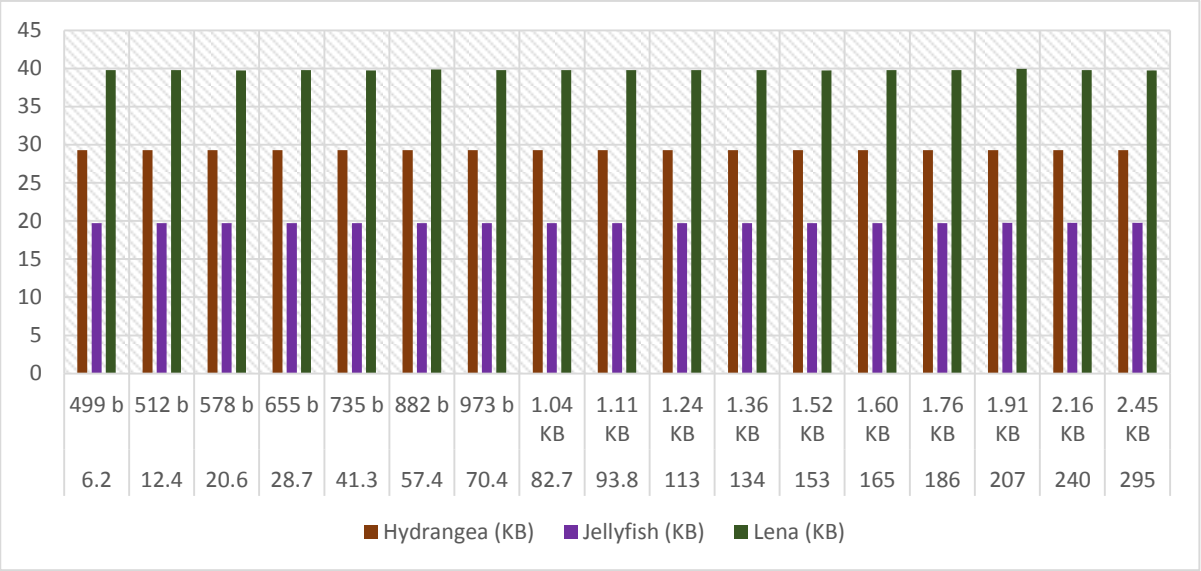

Fig. 3. Graph showing the size of the text file, compressed text file and the stego image

Table 1. Table showing PNSR comparisons between MLSS application, P2P application, and Quickstego application.

Plain Text size	MLSS			P2P			Quick Stego		
	H	***J***	***L***	***H***	***J***	***L***	***H***	***J***	***L***
6.20	67.784	74.003	65.492	64.197	66.387	65.005	68.580	68.389	67.852
12.4	66.762	73.772	67.247	62.111	63.698	62.402	65.602	65.368	64.879
20.6	66.572	73.680	66.907	60.938	61.923	61.436	63.404	63.264	62.684
28.70	65.544	70.791	65.948	59.784	60.310	60.384	61.863	61.767	61.009
41.3	65.291	70.508	65.519	58.441	58.839	58.952	60.304	60.169	59.517
57.4	64.817	69.912	64.818	57.191	57.520	57.671	58.913	58.802	58.127
70.4	65.302	69.920	65.664	56.275	56.642	56.652	57.996	56.586	57.237
82.7	65.365	69.520	65.961	56.092	56.340	56.166	57.293	57.194	56.509
93.8	65.584	51.323	65.934	56.090	56.239	54.608	56.734	56.628	LT
113	65.385	51.321	65.664	53.475	53.936	52.442	LT		
134	65.141	70.447	65.350	51.323	51.707	50.927			
153	65.604	69.249	66.472	50.082	50.443	49.894			
165	64.853	69.947	64.994	49.323	49.776	49.332			
207	65.306	68.592	66.237	47.359	47.847	45.306			
240	65.075	68.792	65.821	44.224	44.306	43.464			

References

[1]. D. Bret, "A detailed look at Steganographic Techniques and their use in an Open System Environment", *SANS Institute Reading Room site, SANS Institute 2002*.

[2]. J. Ashok, Y. Raju, S. Munishankaraiah, and K. Srinivas, "Steganography: An Overview", *International Journal of Engineering Sciences and Technology* Vol. 2(10), pp. 5985-5992, 2010.

[3]. T.J. Ogundele and A.O. Adetunmbi, "Development of Multi-Level System of Steganography" *Journal of Computer Science and Technology* Vol. 13, No 1, pp. 25-31, April 2013.

[4]. K. Amanpreet, D. Renu, and S. Geeta, "A new Image Steganography Based on First Component Alteration Technique", *International of Computer Science and Information Security*, Vol 6, No 3, 2009.

[5]. D. Banerjee, "Assymetric Key Steganography", *International Conference on Information and Electronics Engineering* IPCSIT, vol 6.

[6]. Wikipedia, http://en.wikipedia.org/wiki/steganography, Steganography.

[7]. S. Gandharba, and K. Saroj, "A Technique for secret communication using a new block cipher with dynamic steganography", *International Journal of Security and its Applications* Vol. 6 No 2, 2012.

[8]. K. Rupinder, K. Mandeep, and M. Rahul, "A New Efficient Approach towards Steganography*", International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 2 (2), 673-676, 2011.

[9]. http://www.programmer2programmer.net/live_projects/project_7/steganography.aspx, P2p Live Project 6, "Steganography - Technique to hide information within image file", April 12, 2013.

[10]. http://www.quickcrypto.com/free-steganography-software.html, QuickStego, "Free Steganography Software by QuickCrypto" April 12, 2013.

[11]. Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment", Electronics Letters 44 (13): 800–801.doi:10.1049/el:20080522, 2008.

[12]. http://web.mit.edu/xiphmont/Public/theora/demo7.html MIT.edu, August 13, 2013.

[13]. http://www.varioustopics.com/image-processing/1008462-calculating-rmse-and-psnr-for-color-images.html, "Image Processing Science calculating RMSE and PSNR for color images", August 13, 2013

[14]. www.outguess.org . Xsteg , "Stego detect steganalysis software", October 22, 2014.

[15]. https://www.pantechsolutions.net/blog/matlab-code-for-psnr-and-mse/, "Matlab Code for PSNR and MSE", December 8, 2014.