Journal of Data Analysis and Information Processing, 2015, 3, 168-174
Published Online November 2015 in SciRes. http://www.scirp.org/journal/jdaip
http://dx.doi.org/10.4236/jdaip.2015.34017

Detection of Stego-Images in Communication among the Terrorist Boko-Haram Sect in Nigeria

Owoeye Kolade[1], Ajayi Adedoyin Olayinka[2], Fadugba Sunday[1], Obayomi Adesoji[1], Isinkaye Folasade Olubusola[1]

[1]Ekiti State University, Ado-Ekiti, Nigeria
[2]Federal University of Technology, Akure, Nigeria
Email: kolade_owoeye@yahoo.com, dedoyyin@gmail.com, emmasfad2006@yahoo.com, aaobayomi@yahoo.com, sadeisinkaye@gmail.com

Received 9 August 2015; accepted 21 November 2015; published 24 November 2015

Abstract

Nigeria was listed as a part of terrorist states by United States of America as a result of Islamic group (Boko Haram Sect) attacks and other activities in the nation. It has also been discovered that the group employs "steganographic" schemes as a secure means for transmitting their hidden information to each other via Internet and social networks. The group has killed thousands of people since their increased insurgency in July, 2009. These challenges have affected the nation's foreign policies, political and social economic developments. This research addresses the challenges by employing forensic technique using blind steganalysis approach to detect the presence of the hidden messages in images. Image Quality Metric is employed for extracting the features, and logistic regression is trained as the classifier to predict the stego-images. We show the effectiveness of the method by conducting test and analysis with 319 images varying in size and style. The result shows that the performance of the method is better than other steganalysis methods.

Keywords

Stego, Staganalysis, Logistic Regression, Boko-Haram Sect

1. Introduction

The awareness of insecurity in Nigeria has placed an increasing focus on the need for security of life and properties. According to [1], terrorists are now communicating using steganographic means via the Internet. In Nige-

How to cite this paper: Kolade, O., Olayinka, A.A., Sunday, F., Adesoji, O. and Olubusola, I.F. (2015) Detection of Stego-Images in Communication among the Terrorist Boko-Haram Sect in Nigeria. *Journal of Data Analysis and Information Processing*, **3**, 168-174. http://dx.doi.org/10.4236/jdaip.2015.34017

ria, the Boko Haram Sect also uses similar methods as a means of communicating and sending messages to one another, and they are working with different cyber security expert who are developing a secure steganography system for them [2]. The group proposes to use the means to communicate to each other on the next place of attack which can be in a form of images, video and audio. The term of "steganography" emanated from the Greek, meaning "covered or hidden". Steganography itself is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data. Steganography is the technology of embedding hidden messages. This technique involves sending information to the recipient in a hidden way. The message hiding process can be done to any type of images, such as BMP, GIF and JPEG images. The messages are concealed in such a way that they are hardly noticed. The purpose of steganography is to covert communication to hide messages from a third party [3].

The art of discovering the existence of steganographic data or secret message in an object is called steganalysis. It also refers to as the body of techniques that is designed to distinguish between cover-objects and stego-objects [4]. According to [4], none of the steganographic systems that are known today achieves perfect security, and by this means they all leave hints of embedding in the stegogramme. This gives the steganalyst a useful way to identify whether a secret message exists or not. The major objective of steganalysis is to detect steganography method irrespective of its embedding mechanism. Therefore, universal blind steganalysis is not restricted to a particular algorithm or a class of algorithm [5].

This paper presents an efficient method in detecting steganographic data by employing Image Quality Metrics (IQM) as a means of feature extraction and Logistic Regression analysis for classification. One advantage of this project is that it is able to provide solution to some of steganalysis problems in terms of testing algorithm against payload stego-images and various categories of images such as animals, fruits and natural scenes. Also, the system is able to detect presence of hidden message in cover signal. Another advantage is that the system is able to predict accurately any suspected images irrespective of the algorithm used in embedding process due to the fact that the system is trained with different embedding algorithms, for example, LSB, F5 etc.

2. Related Work

The research on steganalysis started in the late 90's. The idea to use a trained classifier to detect data hiding was first introduced in a paper by [6]. In the paper, image quality metrics were proposed as features and the method was tested on several robust watermarking algorithms as well as Least Significant Bit (LSB) embedding. The work done in [7] described a different set of features based on binary similarity measures between the LSB plane and the second LSB plane capitalizing on the fact that most steganographic schemes use the LSB of image elements as the information-carrying entity. A feature-based steganalysis method for JPEG an image was described and used as a benchmark for comparing JPEG steganographic algorithms and evaluating their embedding mechanisms. The detection method was a linear classifier trained on feature vector corresponding to cover and stego images [8]. The research work in [9] indicated that in general no single feature is capable of differentiating stego and plain images effectively and a combination of features extracted in different domain will be generally more promising.

In [10] features from higher-order moments of distribution of wavelet coefficients and their linear prediction errors from several high-frequency sub-bands were constructed. The same authors also showed that SVMs generally provide better performance as classifiers compared to linear classifiers. Other authors have investigated the problem of blind steganalysis using trained classifiers [11]. Many steganalysis researchers attempt to categorize steganalysis attacks to recover modify or remove the message, based on information available [12].

Dual statistics steganalytic method for detection of LSB embedding in uncompressed formats was introduced in [13]. For high quality images taken with a digital camera or a scanner, the dual statistics steganalysis indicated that the safe bit-rate is less than 0.005 bits per sample, providing a surprisingly stringent upper bound on steganographic capacity of simple LSB embedding.

A universal blind detection scheme that can be applied to any steganographic scheme after proper training on databases of original and cover-images was introduced in [14]. The author used an optimal linear predictor for wavelet coefficients and calculates the first four moments of the distribution of the prediction error. Fisher linear discriminant statistical clustering was used to find a threshold that separates stego-images from cover-images. The work demonstrated the performance on J-Steg, both versions of Outguess, EZ Stego, and LSB embedding. It appeared that the selected statistics was rich enough to cover a very wide range of steganographic methods.

However, the results were reported for a very limited image database of large, high-quality images, and it is not clear how the results will scale to more diverse databases.

A blind steganalysis method was presented in [15], which was based on statistical moments of wavelet histogram characteristic functions and Bayes classifier. Experimental results indicated that the method worked better for LSB, spread spectrum like steganography, F5 and Outguss steganography methods. A universal digital approach to steganalysis for detecting the presence of hidden message embedded within digital images was described in [16]. It was shown that within multiscale, multiorientation image decompositions (e.g. Wavelets), first- and higher-order magnitude and phase statistics were relatively consistent across a broad range of images, but are disturbed by the presence of embedded hidden messages.

Another blind steganalysis method with high detection ratio was proposed based on best wavelet packet decomposition. However, the methods based on wavelet high order statistics could not perform very well on spatial domain steganography such as LSB steganography [17].

Contourlet Based Steganalysis (CBS) was presented in [18], which used statistical moments as well as the log errors between the actual coefficients and predicted coefficients of the contourlet transform as features for analysis. After feature extraction, a nonlinear SVM classifier was applied to classify cover and stego-images. This method converts the image into gray-scale and then processes it. CBS detection rate is very low when message is embedded in medium frequency sub-bands and this idea was used in [19] to develop a new contourlet based steganography algorithm. So if the algorithm in [19] is used to embed the message, then CBS [18] cannot detect successfully. Authors in [20] used steganalytic software Steg Detect in order to test a large sample of images that were downloaded using a web crawler from Usenet and eBay. He used a distributed dictionary attack on suspected stego-images, which were a very small percentages of the images tested, and wasn't able to find any secret messages.

The modern steganography techniques places embedding changes in those regions of images that are hard to model and hence increasingly more complex statistical descriptors of covers that are required to capture a large number of dependencies among cover elements that might be disturbed by embedding.

Much works have been done in the literature but need for better and efficient method in term of high prediction rate for further development of steganalysis necessary. Therefore, this paper adopted IQM as a method for feature extraction technique.

3. Theoretical Framework

319 images were tested and analyzed. Messages were embedded to 169 gray scale images using four known steganography software which are VLS (Virtual Laboratory Steganography), with different embedding algorithms which enable our system to learn and predict accurately any suspected images irrespective of the algorithms used in their embedding process. Thereafter, feature extraction process took place and logistic regression is trained as the classifier to predict the stego-images. The table in the appendix showed the data analysis with IQM functions used for the images.

3.1. Training Process

The training process block diagram is as represented in **Figure 1** below.

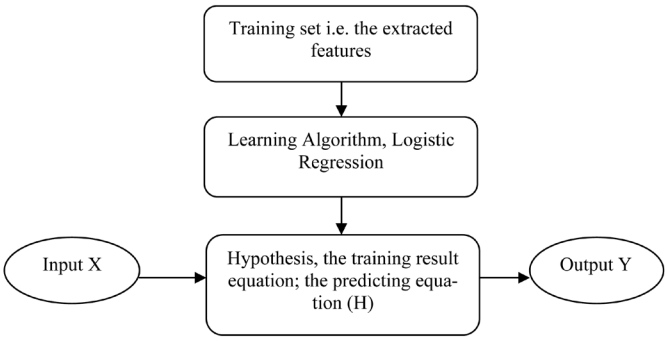

Figure 1. Block diagram of the training process.

From the block diagram, the training set is the features extracted using the image quality measures (IQM). X is the input features to the hypothesis that is, to the predicting equation while the output Y is the result generated from the predicting equation based on the input features. The result in this case is either 1 representing stego-image or 0 representing cover image.

Let $x(i)$ denote input variable *i.e.* extracted features;

Let $y(i)$ denote output variable or the targeted variable;

y can only take on two values 0 and 1, that is; y! {0,1};

$(x(i), y(i))$ denote the training examples.

3.2. Steganalytic Classifier

Logistic regression analysis is used on the selected features generated through Image Quality Measures (IQM) to build an optimal classifier using a set of test images and an original image. The idea is that the distance between a two cover images is less than the distance between a cover image and a stego-image. That is

$$\left(C - C_d\right) < \left(S - S_d\right) \tag{1}$$

where,

C represents Cover image;

C_d represents distortion of the cover image;

S represents a stego-image;

S_d represents distortion of the stego-image.

3.3. Logistic Regression

The focus here is on the binary classification problem in which y can take on only two values, 0 (cover-image) and 1 (stego-image). 0 is also called the negative class, and 1 the positive class, and they are sometimes also denoted by the symbols "–" and "+".

Let the predicting equation, that is, the hypothesis be denoted as $hi^Q x^V$, which is written as

$$hi^Q x^V = g^Q i^T x^V = \frac{1}{1+\mathrm{e}^{-i^T x}} \tag{2}$$

where $g^Q z^V = \dfrac{1}{1+\mathrm{e}^{-z}}$ is called the logistic function or the sigmoid function. i denotes the learning parameters. T is the intercept from the linear regression equation added to the regression coefficient multiplied by some value of the predictor x.

4. Case Processing Summary

The features extracted from 150 cover images and 169 stego-images were trained on Logistic Regression classifier using SPSS. **Table 1** below shows the result of the training process.

Table 2 shows the variable(s) entered in Step 1 (**Table 3**): MSR, PSNR, MNC, AD, SC, MD, NAE, SD.

Structural Content (SC) defines the closeness between two images can be quantified in terms of correlation function. These measures measure the similarity between two images; hence in this sense they are complementary to the difference-based measures.

$$\mathrm{SC} = \sum_{j=1}^{M}\sum_{k=1}^{N} X_{j,k}^2 \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N} X'^2_{j,k} \tag{3}$$

where M and N are the dimension of the image, $x_{j,k}$ is the original image and $x'_{j,k}$ is the distorted image

MSE is the Mean Square Error. It is defined as

$$\mathrm{MSE} = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(X_{j,k} - X'_{j,k}\right)^2 \tag{4}$$

where M and N are the dimension of the image, $x_{j,k}$ is the original image and $x'_{j,k}$ is the distorted image.

AD is the Average Difference, given by

Table 1. Result of the training process.

	Unweighted Cases	*N*	Percentage
Selected Cases	Included in Analysis	319	100.0
	Missing Cases	0	0.0
	Total	319	100.0
Unselected Cases		0	0
	Total	319	100.0

Table 2. Variables in the equation.

	B	**S.E.**	**Wald**	**df**	**Sig.**	**Exp(B)**
MSR	−0.519	9850.349	0.000	1	10.000	0.595
PSNR	−0.298	0.275	10.173	1	0.279	0.742
MNC	1230.551	930.104	10.761	1	0.185	40.543E53
AD	−0.570	0.568	10.009	1	0.315	0.565
SC	900.810	520.868	20.950	1	0.086	20.742E39
MD	0.008	0.005	20.425	1	0.119	10.008
NAE	380.275	160.399	50.448	1	0.020	40.195E16
SD	0.516	9850.349	0.000	1	10.000	10.676
CONSTANT	−2090.710	1440.044	20.120	1	0.145	0.000

Table 3. Model summary.

Step	−2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	414.005[a]	0.081	0.109

$$\mathrm{AD} = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(X_{j,k} - X'_{j,k}\right)\Big/MN \tag{5}$$

where *M* and *N* are the dimension of the image, $x_{j,k}$ is the original image and $x'_{j,k}$ is the distorted image.

PSNR is Peak Signal to Noise Ratio. It is used to find the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is commonly used to measure the quality of reconstruction of lossy compression codecs especially for image compression. PSNR is given by

$$\mathrm{PSNR} = 10\log\frac{255^2}{\mathrm{MSE}} \tag{6}$$

MD is the Maximum Difference, given by

$$\mathrm{MD} = \mathrm{Max}\left(\left|X_{j,k} - X'_{j,k}\right|\right) \tag{7}$$

SD is the Spectral Distance, while NAE is the Normalized Absolute Error, given by

$$\mathrm{NAE} = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(\left|X_{j,k} - X'_{j,k}\right|\right)\Big/\sum_{j=1}^{M}\sum_{k=1}^{N}\left(\left|X_{j,k}\right|\right) \tag{8}$$

Estimation terminated at iteration number 20 because maximum iterations have been reached. Final solution cannot be found.

Hypothesis

General hypothesis (predicting equation)

$$H = 1/\left(1+\mathrm{e}^{-Y}\right) \tag{9}$$

The hypothesis generated from the trained data is

$$\begin{aligned} Y = {} & -209.710 + \left(-0.519 * MSR\right) + \left(-0.298 * PSNR\right) + \left(123.551 * MNC\right) + \left(-0.570 * AD\right) \\ & + \left(90.810 * SC\right) + \left(0.008 * MD\right) + \left(38.275 * NAE\right) + \left(0.516 * SD\right) \end{aligned} \tag{10}$$

The above equation is the predictive equation.

5. Result

The result after testing the system with 319 images is shown in **Table 4** below.

The result of the testing in **Table 4** show that the system achieved 58.9% detection rate, despite training the system with a low images (319) compare to [3] that was trained with 12,200 images. This means if the system was trained with more images, it will achieve very high prediction rate.

The result of this research work is compared with work done in [16] and [8] and the results are presented below in **Table 5**.

The result of the table above show that the system implemented in this project has a high prediction rate compare with WBS [16] and FBS [8].

6. Summary and Conclusion

The approach in this method has provided an easy method for steganalysis and robustness in terms of testing the system against different payload stego-images. We are able to show the effectiveness of the method by conducting test and analysis with 319 images varying in size and style. Messages are embedded to 169 gray scale images using four known steganography softwares which are VLS (Virtual Laboratory Steganography), SecretLayer, QuickStego and OpenStego with different embedding algorithms which enable our system to learn and predict accurately any suspected images irrespective of the algorithms used in their embedding process. Thereafter, feature extraction process takes place and logistic regression is trained as the classifier to predict the stego-images. Finally, our method is able to achieve 58.9% detection rate, despite training the system with a low images (319) compare to existing methods with that were trained with 12,200 images. This means that our method is more efficient.

The output of this paper is recommended to Ministry of Defense to serve as part of reference effort necessary

Table 4. Testing result-classification table.

	Observed Y	Predicted Y		Percentage Correct
		0	1	
Step 1	0	57	93	38.0
	1	38	131	77.5
	Overall Percentage			58.9

Table 5. Result comparison.

Secret Data Size(bits)	Steganalysis Method	Average detection Accuracy (%)
5000	WBS	51
	FBS	53
	This Research	58.9

in curbing the Boko-Haram insurgency menace in the country.

References

[1] Kelley, J. (2001) Terror Groups Hide behind Web Encryption. USA Today. http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

[2] Victor, O., Waziri, A., Abraham, O., Shafi, I. and Muhammad, A. (2012) Steganography and Its Applications in Information Dessimilation on the Web Using Images as Security Embedment: A Wavelet Approach. *International Journal of Computer and Information Technology*, **1**, 194-202.

[3] (2006) Wikipedia. http://www.wikipedia.com/

[4] Bateman, P. (2008) Image Steganography and Steganalysis. Department of Computing Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, 6.

[5] Tzschoppe, R. and Bauml, R. (2003) Steganographic System Based on Higher-Order Statistics. *SPIE*, **2003**.

[6] Avcibas, I., Memon, N. and Sankur, B. (2001) Steganalysis Using Image Quality Metrics. *Proceedings of SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents*, **4314**, 523-531.

[7] Avcibas, I., Sankur, B. and Memon, N. (2002) Image Steganalysis with Binary Similarity Measures. *Proceedings of International Conference on Image Processing*, **3**, 645-648. http://dx.doi.org/10.1109/ICIP.2002.1039053

[8] Fridrich, J. (2004) Feature-Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes. *Lecture Notes in Computer Science*, **3200**, 67-81. http://dx.doi.org/10.1007/978-3-540-30114-1_6

[9] Lie, W.N. and, Lin, G.S. (2005) A Feature-Based Classification Technique for Blind Image Steganalysis. *IEEE Transactions Multimeda*, **7**, 1007-1083. http://dx.doi.org/10.1109/TMM.2005.858377

[10] Lyu, S.W. and Farid, H. (2006) Steganalysis Using Higher-Order Image Statistics. *IEEE Transactions on Information Forensics and Security*, **1**, 111-119. http://dx.doi.org/10.1109/TIFS.2005.863485

[11] Tzschoppe, R., Auml, R.B., Huber, J.B. and Kaup, A. (2003) Steganographic System Based on Higher-Order Statistics. *Proceedings of SPIE Electronic Imaging*, *Security*, *Steganography*, and *Watermarking of Multimedia Contents V*, Santa Clara, 156-166. http://dx.doi.org/10.1117/12.477301

[12] Johnson, N.F. and Jajodia, S. (1998) Exploring Steganography: Seeing the Unseen. *Computer*, **31**, 26-34. http://dx.doi.org/10.1109/MC.1998.4655281

[13] Fridrich, J., Goljan, M. and Du, R. (2001) Reliable Detection of LSB Steganography in Color and Grayscale Images. *Proceedings of* 2001 *ACM Workshop on Multimedia and Security*: *New Challenges*, 27-30. http://dx.doi.org/10.1145/1232454.1232466

[14] Farid, H. (2001) Detecting Steganographic Message in Digital Images. Technical Report, TR2001-412, Dartmouth College, New Hampshire.

[15] Xuan, G.R., Sh,i Y.Q. and Gao, J.J. (2005) Steganalysis Based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions. *Proceedings of 7th International Information Hiding Workshop*, *LNCS*, **3727**, 262-277. http://dx.doi.org/10.1007/11558859_20

[16] Lyu, S.W. and Farid, H. (2006) Steganalysis Using Higher-Order Image Statistics. *IEEE Transactions on Information Forensics and Security*, **1**, 111-119. http://dx.doi.org/10.1109/TIFS.2005.863485

[17] Luo, W., Huang, F. and Huang, J. (2010) Edge Adaptive Image Steganography Based on LSB Matching Revisited. *IEEE Transactions on Information Forensics and Security*, **5**, 201-214. http://dx.doi.org/10.1109/TIFS.2010.2041812

[18] Sajedi, H. and Jamzad, M. (2008) A Steganalysis Method Based on Contourlet Transform Coefficients. *International Conference of Intelligent Information Hiding and Multimedia Signal Processing* (*IIHMSP*'08), Harbin, 15-17 August, 245-248. http://dx.doi.org/10.1109/IIH-MSP.2008.11

[19] Sajedi, H. and Jamzad, M. (2009) ContSteg: Contourlet-Based Steganography Method. *Wireless Sensor Network*, **1**, 163-170.

[20] Provos, N. and Honeyman, P. (2002) Detecting Steganographic Contenton the Internet. *Internet Society*: *Network and Distributed System Security Symposium* (*ISOC NDSS*' *February* 2002), San Diego http://www.citi.umich.edu/u/provos/papers/detecting.pdf