A Formulation of Conditional States on Steganalysis Approach

ROSHIDI DIN[1], ZHAMRI CHE ANI[3]
School of Computing
College of Arts and Sciences
Universiti Utara Malaysia (UUM)
06000 Sintok, Kedah,
MALAYSIA
roshidi@uum.edu.my[1], zhamri@uum.edu.my[3]

AZMAN SAMSUDIN[2]
School of Computer Sciences
Universiti Sains Malaysia (USM)
11800 Minden, Pulau Pinang,
MALAYSIA
azman@cs.usm.my[2]

Abstract— In this paper, we present a consolidated formulation of conditional states from the perspective of steganalysis approach. It has been identified that the conditional states used in steganalysis approach include hypothesis testing, gaussion distribution, hidden markov model and vector analysis space. The main objective of this paper is to find the best approach to fit in using mathematical formulation for steganalytic system based on these conditional states. It is found that there is a boundary of solution between the steganalytic system and analyzed message.

Key-Words:- Steganalysis, Steganalytic System, Steganography

1 Introduction

One of the latest discussions in information hiding area is the steganology field. Steganology is the art and science of concealing and detecting of information through distrusted communication channels. The study area is dealing with the writing of hidden messages and the discovery of the existence of such hidden messages. Unlike cryptology, which is utilized the encrypted messages and decrypted messages of secret writing which rendering the cover messages completely meaningless, steganology keeps the cover messages perceptually unchanged after concealing and detecting of the covered writing. It is a good complement to cryptology and has played a promising role in the e-political and e-military matters from medieval times through the 20th century. In fact, there are two (2) main branches of steganology:

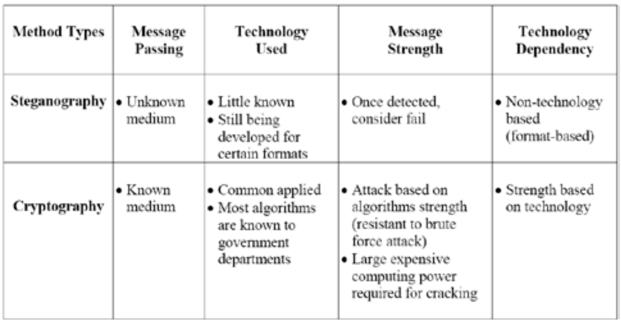
- *Steganography*, is concerned with avoiding the suspicion of hidden messages in a manipulated text
- *Steganalysis*, is concerned with discovering and rendering useless messages such as covert messages in given text

Various applications have been implemented in steganology field which are steganography [1, 2, 3] and steganalysis [4, 5].

Nowadays, with the rapid development of science and technology, steganography has become one of the major disciplines in the area of hidden information research. Steganography plays an important role in protecting the security of all documents over the Internet in this era of terabit networks such as secret data transactions, e-commerce documents protection, digital copyright protection, information identification, information control, and security bills. The main goal of steganography is to convey message under cover, concealing the very existence of information exchange. As a ‘covered writing’, steganography uses a covert communication between two parties whose existence is unknown to a possible attacker. If this is done properly, the exchanged messages should not arouse any suspicion since the information passed is an innocent looking message which does not require any secret key as part of its information hiding process. This can be done in many ways such as inclusion of line break characters, and multiple spacing that represents a hidden message. It can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

Steganography also differs from cryptography, which does not conceal the communication itself but only scrambles the data to prevent eavesdroppers understanding the content. Cryptography involves various methods and implementations. On the other hand, cryptography is the study of secret writing or cryptograms. Cryptography scrambles messages so they cannot be understood and for a purpose. In short, cryptography is about protecting the content of messages; steganography is about concealing the existing messages. Table 1 below shows the advantages and disadvantages of both technologies.

Table1. Comparison between steganography and cryptography



Method Types	Message Passing	Technology Used	Message Strength	Technology Dependency
Steganography	• Unknown medium	• Little known • Still being developed for certain formats	• Once detected, consider fail	• Non-technology based (format-based)
Cryptography	• Known medium	• Common applied • Most algorithms are known to government departments	• Attack based on algorithms strength (resistant to brute force attack) • Large expensive computing power required for cracking	• Strength based on technology

1.1 Steganalysis

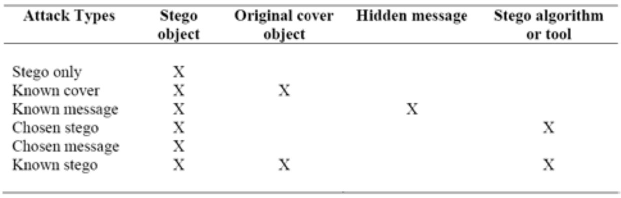
Research reveals that many of the new directions in steganography originated from attack analyses are called steganalysis. The process of analyzing steganographic protocols is carried out in order to detect and extract hidden messages known as stego message. Generally, steganalysis starts with several suspected information streams but is uncertain whether any of the information streams contains stego messages. While the goal of steganography is to avoid suspicion to hidden messages in other data, steganalysis aims to discover and render useless messages such as covert messages in a given text or data. Thus, steganalysis is the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes. It is the art of discovering and rendering useless covert messages.

Generally, steganalysis techniques could be classified into two broad categories namely specific steganalysis and universal steganalysis [6]. Until recently, the technology of steganalysis system becomes more sophisticated and it has rapidly being implemented into numerous practices [7]. It can be identified into four approaches [8] which are:

- *Supervised learning detection*
- *Blind identification*
- *Parametrical statistical detection*
- *Hybrid techniques*

Besides, it has been known that there are six types of parameters used in steganalysis system [9, 10, 11], and they are shown in Table 2.

Table 2. Types of steganographic attacks



Attack Types	Stego object	Original cover object	Hidden message	Stego algorithm or tool
Stego only	X			
Known cover	X	X		
Known message	X		X	
Chosen stego	X			X
Chosen message	X			
Known stego	X	X		X

1.2 Steganalysis Model

The processes of steganography and steganalysis can be represented by *Prisoner's Problem* [12]. Alice and Bob are locked up in separate cells far apart from each other. They are allowed to communicate by means of sending messages via Wendy as a gatekeeper [13] who does not suspect such communication is taking place. Wendy who plays the role of the adversary will break all communication that comes to her. If Wendy detects any sign of conspiracy, she will suppress all the messages. Alice and Bob are well aware of these facts. Thus, Alice is trying to send a hidden message *M*, within a cover message *C*, which involves a stego key *K* through an embedding process known as *S*. The first step is applying the invertible function $e: \{M, C\} \rightarrow S$. Then, Alice can map a hidden message *M* to a stego message *S*, using key *K* through $e(M, C) = S$. Since *S* is a stego message, Wendy will not find it suspicious, and since the function is invertible, Bob will be able to compute $e^{-1}(S) = \{M, C\}$ in order to reconstruct the hidden message *M* and cover message *C* with a stego key *K*.

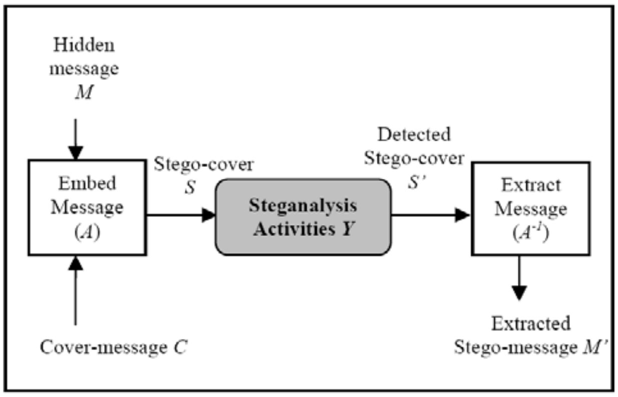


Fig. 1 A black box process on steganaytic system

This process might use a function $d: S*C*K \rightarrow M$ to decode the stego message. Related to this fact, Wendy as a good gatekeeper must monitor all the communication between Alice and Bob which is shown in Fig.1. In doing so, Wendy can take either of these actions, or both;

- *Passive Gatekeeper* – only detects the presence/absence of hidden message *M* in an observed message (stego-cover) *S* and identifies the stego-embedding algorithm/key.
- *Active Gatekeeper* – tries to recover the stego message *M'*, including embedded message length, locations of the hidden message *M*, stego key used in embedding algorithm, some parameters of the stego-embedding algorithm and finally extract A^{-1} (if possible) the stego message *M'*.

If any of the hidden communication is taking place between Alice and Bob, Wendy has the capability to extract or at least to detect the sign of hidden communication. Thus, Wendy needs a good formulation technique for steganalytic system in order to analyze the exchange message of the communication. Clearly, there are at least five challenges for Wendy as a gatekeeper need to be considered and these challenges are summarized below.

- *Analyzed message may or may not have hidden data embedded into them*
- *Hidden data may or may not have been encrypted before inserted into the analyze message*
- *Analyzed message may or may not have noise or encoded data into them*
- *Analyzed message may or may not possible to fully recover or extract the hidden data*
- *Analyzing message is very time consuming process*

From the theoretical point of view, the main idea of this paper is to address some of the conditional states of these challenges with a mathematical formulation in the steganalysis domain. Our primary goal is to find the *bestfit* method for the gatekeeper in order to detect any suspicious or hidden data from analyzed message. Note that, we assume that both steganographers (Alice and Bob) and gatekeeper (Wendy) have the same capability to exploit any statistical features available on their models.

This paper is organized as follows. Section II deals with the four conditional states of steganalytic system such as hypothesis testing, gaussion distribution, hidden markov model and vector analysis space. The Concluding remarks are given in Section III.

2 Conditional States On Steganalysis Approach

The fact of steganalytic system conditional is that the more focused a steganalysis conditional is on a specific steganalytic system technique the less its generalization capability is. On the other hand, a very general conditional state may not produce acceptable performance of a specific steganalysis technique. Usually, the steganalysis techniques have been influenced by the strength of the chosen steganalytic system model. Therefore, choosing the right model of steganalytic system itself is an open research problem.

The fundamental problem in coming up with a steganalytic model is that both the steganographers and the gatekeepers are always improving their techniques. Thus, to obtain a fair analysis, we have to assume that both parties are exploiting the same statistical features available on their models. Based on this assumption, there are four conditional states that can be illustrated on the model of steganalytic system such as *Hypothesis Testing*, *Gaussion Distribution*, *Hidden Markov Model* and *Vector Analysis Space.*

2.1 Hypothesis Testing

One of the conditional states of steganalytic system can be illustrated through the conditional entropy based on information theory [14]. Let's say

$$H(S|C) = H(C|S) = 0 \qquad (1)$$

is the conditional uncertainty of *H* on stego-cover *S* when knowing cover-message *C*, is equal to the conditional uncertainty of *H* on cover-message *C* when knowing stego-cover *S* are equal to 0. Equation (1) represents the state where the analyzed message is not having embedded information. Then,

$$H(S|C) = H(C|S) > 0 \qquad (2)$$

is the conditional uncertainty of stego-cover *S* when knowing cover-message *C* is equal to the conditional uncertainty of cover-message *C* when knowing stego-cover *S* which is more than 0. Equation (2) represents the state where the analyzed message is having embedded information. Therefore, the ultimate condition for steganography system as a *perfectly secure system* (during transforming information) is a conditional entropy of $H(S|C) = H(C|S) = 0$ [15]. However, the perfectly secure steganography system is impossible to achieve when both stego-cover *S* and cover-message *C* are known to Alice. Another conditional state of analyzed message from information theory is a conditional of parameter changes. Let's say, a value of parameter θ would change based on the message embedding process within a time k. Thus the steganalysis problem is to detect any change in parameter θ and estimate the changes time k_0. This state can be expressed as

$$H_0 : \theta = \theta_0 \text{ when } k < k_0$$
$$H_1 : \theta = \theta_1 \text{ when } k \ >= k_0 \tag{3}$$

where hypothesis H_o represents that no embedded message has been found while H_1 represents that an embedded message has been found in the analyzed message. This hypothesis can be implemented either using parameter values that are completely known or the parameter values that are partially known [16]. Hence, based on equation (3), the hypothesis parameters Y_k can be represented as

$$H_0 : Y_k \ = X_k + K \sim P_0$$
$$H_1 : Y_k \ = X_k \quad \sim P_1 \tag{4}$$

Normally, this hypothesis can be analyzed through performance analysis on conditional state known as *Receiver Operating Characteristics* (ROC). The ROC is used as a trade-off of false alarm probability with the probability of detection by the detectors with several characteristics function [17] which;

- represents the achievable performance of the steganalysis detectors,
- uses relative entropy between the cover message and the stego message probability distribution, and
- employs the minimum probability of error criterion.

the false alarm probability α_k can be optimally traded-off with the probability of detection (miss probability) β_k by using the receiver operating characteristic function. Thus, based on equation (4), there are two possible error probabilities [18] that need to be considered while testing for the hypothesis y_k as

$$\alpha_k = P_0$$
$$\beta_k = P_1 \tag{5}$$

From the equation (5), it shows that Wendy as a gatekeeper can use the *Neyman-Pearson* detector to yield the highest probability of detection for a given false alarm probability α_k since the probability of detection β_k has increased by K value. Thus, K value can be considered as a measure of the distance between the probability distribution under H_0 and H_1. Clearly, the higher the K value is, the easier it is to distinguish between H_0 and H_1 by Wendy.

Another performance analysis is the random variable test which represents fixed false alarm and missed error probabilities known as *Sequential Probability Ratio Test*. This can be used as a detector with two thresholds identified as h and - γ [19]. Thus, based on these thresholds, *Cumulative Sum* (CUSUM) S^k_1 will be computed and used for identifying change points in order to detect the location and length of messages embedded on the analyzed message as

$$S^k_1 = \ \Sigma^i s_i \tag{6}$$

where

$$S^k_1 \geq h \ \ accept\ H_0$$
$$S^k_1 < -\gamma\, accept\ H_1$$

From equation (6), H_1 is accepted when CUSUM test is greater than h and H_0 is also accepted when CUSUM test is greater than - γ. Thus, it can be said that the steganalysis detector performance depends on these two thresholds detection. Now, consider that false alarm probability (probability of accepting H_1) as α and missed error probabilities (probability of rejecting H_1) as β, then the optimal upper threshold value can be stated as

$$h = \text{In} \ \ \frac{1-\alpha}{\beta} \tag{7}$$

when S^k_1 is taken across threshold h, CUSUM test detect a location range of embedded message which is from parameter θ changing to parameter θ_1 and back to parameter θ. Thus, this symmetry view can be shown from threshold h to threshold h_1. It will then detect hypothesis H_0 as

$$h_1 = \text{In} \ \ \frac{1-\alpha}{\beta} \tag{8}$$

However, this will happen only if the CUSUM test has crossed the threshold h. Another problem is that θ_o and θ_1 values are completely unknown in real implementation.

2.2 Gaussion Distribution

Another conditional state of the steganography system that can be illustrated is through Gaussion distribution curve. Assuming that,

S	*stego-cover*
M	*hidden message*
C	*cover-message*
f_e	*embedding message*

the embedding process f_e of hiding original message M should exploit the embedding key K with the preprocessing random characteristics r (such as white noise) on cover-message C as f_p known as actual cover C_r

$$\begin{aligned} S &= f_e(C, M, K) \\ S &= f_p(C, r) + M + K \\ S &= C_r + M + K \end{aligned} \tag{9}$$

Therefore, Wendy as a gatekeeper must not know that the analyzed message is a stego-cover. It means that the gatekeeper cannot decide whether the analyzed message contains cover-message or not. However, hidden message M is statistically different from the cover-message C. Thus, this statistical difference measure can be used by gatekeeper's detector in detecting the stego message S. At the same time, gatekeeper can also use this information to decide the presence/absence of a hidden message. Based on the decision there could be attempts to extract the hidden message, if possible. Thus, from conditional state of steganography system, the only knowledge available is that

$$y(k) = s(k) + \alpha w(k),\ k = 1, 2, \ldots, N \tag{10}$$

state that

$y(k)$	*analyzed message*
$s(k)$	*cover-message*
$w(k)$	*stego-cover*
α	*message strength* $\alpha > 0$ *based on perceptual characteristics, robustness properties etc.*

It can be assumed that the signal distribution of analyzed message $y(k)$ and common transform coefficient distribution of cover-message $w(k)$ is justified as Gaussion distribution. Hence,

$$\begin{aligned} &y(k) = s(k) + \alpha w(k), \\ &w(k) = 0 \\ &y(k) = s(k) \ \textit{no hidden message} \end{aligned} \tag{11}$$

As passive gatekeeper, if stego-cover $w(k)$ is equal to zero then it can be identified that cover-message $s(k)$ does not carry a hidden message M. Otherwise, for active gatekeeper it is directly subtracting cover-message $s(k)$ from analyzed message $y(k)$ in order to extract the hidden message M such as

$$\begin{aligned} y(k) &= s(k) + \alpha w(k), \\ aw(k) &= y(k) - s(k) \ \textit{message extracted} \end{aligned} \tag{12}$$

However, most of the analyzed message related features are non-Gaussion. Meanwhile, the simple subtraction scheme does not perform well on huge sizes of analyzed message. Therefore it may be able to exploit higher order statistics during steganalysis because higher order statistics is estimated to be more reliable for larger message sizes. Thus, the extraction process of cover-message $s(k)$ from analyzed message $y(k)$ as given in equation (10) is clearly a statistical regression problem. Specifically, once the estimation of analyzed message $s(k)$ is obtained there are two choices;

- simply subtract this estimation from analyzed message $y(k)$ to obtain an estimation of stego-cover $w(k)$ or
- attempt to formulate blind inverse computation on stego function using higher order statistics.

Based on equation (5) and equation (10) which are obtained as discussed above, the idea is to assume that there are two copies of stego function analyzed message available to the steganalyst be $y_1(k)$ and $y_2(k)$ which are formulated as

$$\begin{aligned} y_1(k) &= \alpha_1 s(k) + \alpha_2 w(k),\ k = 1, 2, \ldots, N \\ y_2(k) &= \beta_1 s(k) + \beta_2 w(k),\ k = 1, 2, \ldots, N \end{aligned} \tag{13}$$

Thus, these two copies of stego function can be in discovering the solution based on blind source separation problem if an *identifiability condition* [20] has been fulfilled:

- At most one of $s(k)$ or $w(k)$ is non-Gaussion
- The matrix A must be of full column-rank

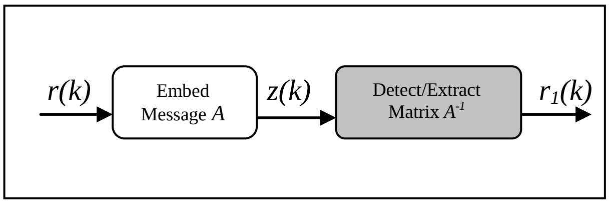


Fig. 2 Blind system identification problem [21]

The steganalysis problem is to find a linear transformation of inferring A from $z(k)$ as shown in Fig. 2. If A^{-1} can be identified, hence we can obtain $r(k)$ from A^{-1} $z(k)$ such as

$$z(k) = \begin{pmatrix} y_1(k) \\ y_2(k) \end{pmatrix} = Ar\,(k) \qquad (14)$$

Assuming that

z(k)	*vector of stego message*
A	*strength matrix*
r(k)	*vector components { α, β } of cover message and secret message*

However, there are several criticisms of this idea in actual steganalysis environment, such as;

- Sender and receiver may not use the same key (embed and extract) for two or more stego messages especially in public key steganography (PKS) environment.
- Sender and receiver may not use the same cover message, the same key and the same secret message for at least two stego messages.
- The stego message cannot be detected because most of the stego message distribution is a non-linear transform distribution.
- A Gaussion vector cannot be manipulated because stego messages's related features are non-Gaussion vector pattern.
- Most of the secret message and cover message types are statistically independent.

2.3 Hidden Markov Model (HMM)

One of the condition states of steganography system that can be represented is through Hidden Markov Model (HMM). This model is useful for formulating and solving steganalysis problems for different types of containers in one unified standard because it is used in many applications of image [22], video [23], sound [24] and text processing [25]. Here, steganalysis is considered as a statistical model to check the changes of statistical properties on analyzed message such as histogram values or internal correlation of messages container [26] based on HMM [27]. Let's consider that;

- the containers are produced by a random source *X* with distribution *PX*
- the secret messages and keys are produced by random sources *M* and *K*

It can be assumed that Wendy partly knows the distribution of *X* on analyzed message *Y*. She also knows little information *θ* of *M* and *K* that can be stated as *θ (m; k*). Thus, based on this conditional state, Wendy can model the embedding process of secret message in conditional distribution *P θ(m)* such as

$$P\,\theta\,(m) = \sum_{k\,\in} PX(k)\, P\,\theta\,(m|k) \qquad (15)$$

Thus for all possible *θ* values,

$$\text{if } m = k \text{ then } P\,\theta\,(m|k) = 1$$
$$\text{if } m \neq m \text{ then } P\,\theta\,(m|k) = 0$$

Hence, the steganalysis problems that can be manipulated by Wendy are:

- *Passive gatekeeper*: Tries to distinguish whether there is an existence of secret information *θ* or not and may try to acquire some information about secret messages *m* or secret keys *k* inside analyzed message *Y.*
- *Active gatekeeper*: Not only concerned on the questions related to the strength of steganography system that sender uses but also in such a way be able to formulate the problem of evaluating secret messages *m* when secret keys *k* is used for spreading secret messages *m* over secret keys *k.* She is also concerned on the problems of evaluating secret key, k.

By applying the HMM, Wendy's problems can be handled when the container distribution has utilized a markov properties (such as a markov chain, a markov process or a markov field) in order to describe the internal correlation of *k.* Thus, based on equation (15) with the parameters λ = {*q*, *r*, *s*} of the HMM, it can be assumed that,

$$\begin{aligned} P(Y{=}m) &= P(m \mid \lambda) \\ &= \Sigma\, P(k \mid r, q)\, P(m \mid k, s) \\ &= \Sigma\, qk_1\, sk_1m_1\, rk_1k_2\, sk_2m_2 \ldots rk_{T-1}k_T\, sk_Tm_T \quad (16) \end{aligned}$$

Wendy does not have to know the exact distribution on *K* but only suggests that it is a markov property of the analyzed message. By maximizing *P(m | λ)* using with EM (*Expectation Modification*) algorithm or *Viterbi algorithm,* this model can not only predict the parameter values of the conditional distribution *P(m | k)* of hidden message, but also find parameters of prior distribution of the analyzed message. However, the Markov field model is better than Markov chain model in stimulating analyzed message.

2.4 Vector Space Analysis and Receive Operating Characteristic

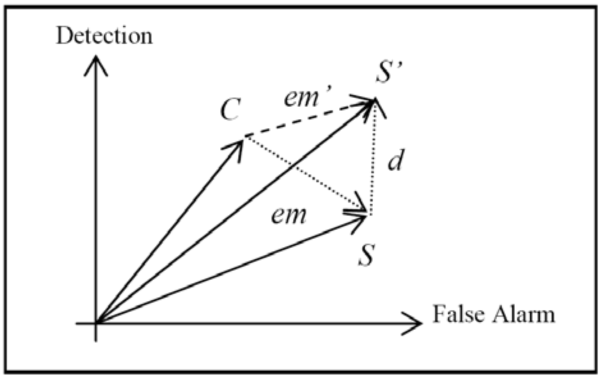


Fig. 3 The embedding and extraction processes of steganography system

One of the possible ways to analyze a steganography system is to use a vector space method [28]. This method states that the process of analyzing message is based on embedding intensity, detection intensity and robustness through a geometrical *n*-dimension as shown in Fig. 3. Assuming that,

C	*cover-message*
S	*stego-cover*
S'	*detected-stego-cover*
d	*detection*
em	*embedding message*
em'	*extraction message*

A message embedding is the vector from point *C* to point *S* which can be identified as $S = C + ew$ and an extraction message is the vector from point *C* to point *S'* which can be presented as $S' = C + ew'$ whereas a message detection can be assumed as $S' = S + d$. Thus, Wendy can use a vector *d* from point *S* to point *S'* to detect the suspected stego-cover through *n*-dimension vectors to analyze a process of any steganography system as shown in Fig. 4.

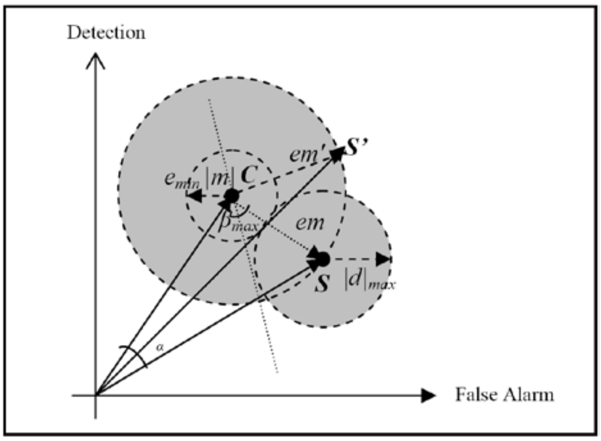


Fig. 4 An analysis of steganography system

Stated that,

$$S' = C + em'$$
$$em' = S' - C \quad (17)$$

Then,

$$S' = S + d$$
$$d = S' - S \quad (18)$$

So that,

$$|d|_{max} = C + em' - S \quad (19)$$

Assuming that, a minimum message embedding is $e_{min}|m|$, the angle β is a difference between *em* and *em'* weights and *L* is a length of cover *C*. Because the detection comes from Wendy, the steganography system try to resist a maximum detection range $|d|_{max}$ as possible as it can through the angle between *em* and the straight line from point *C* and tangents with sphere R as β_{max}. Thus, a detection range can be avoided.

However, Wendy can try to find the range of β_{max} angle based on *n*-dimension space theorem, which can be denoted as $\sqrt{((2\ |C|\ (1 - \cos\alpha)\ (|C| - L) + L_2)}$. Thus, the existence of stego-cover can be identified by steganalytic system when

$$e_{min}|m| < \beta_{max}$$
$$e_{min}|m| < \sqrt{((2\ |C|\ (1 - \cos\alpha)\ (|C| - L\ ) + L_2))} \quad (20)$$

Hence, the steganography system should hide the least embedded message as well as *stego-key K*, since it may be enough for Wendy to learn only a small amount of information about the embedded message to conclude that Alice and Bob are conspiring something. Thus, one of the steganalysis detector mechanisms that can be used by Wendy is based on *Receiver Operating Characteristic* (ROC) plot of α versus β which represents the capability of steganalysis detector performance. Assuming that,

C	*cover-message*
S	*stego-cover*
S'	*detected-stego-cover*
α	*probability of false alarm*
β	*probability of detection*
α and *β*,	*detector dependent values*

It can be assumed that α is the probability of hidden message is detected when no message is predicted and β is the probability of hidden message detected when no existing message is predicted. Thus, a steganalysis detector performance can be measured through the probability of steganalysis error P_e [17];

$$P_e = (1 - \textit{prob. of detection})\ P(\textit{message detected}) + (\textit{prob. of false alarm})\ P(\textit{no. message})$$

$$P_e = (1 - \beta)\ P(\textit{message detected}) + \alpha\ P(\textit{no. message}) \qquad (21)$$

If Wendy does not justify whether a message is embedded or not, she can assume that

$$P\ (\textit{message detected}) = P\ (\textit{no message}) = 0.5$$

thus,

$$P_e = (1 - \beta)P(\ 0.5) + \alpha P(0.5)$$
$$P_e = 0.5\ [(1 - \beta) + \alpha] \qquad (22)$$

However, steganography system requires more than that. The stego-cover *S*, generated by most embedding schemes, resembles a sequence of random bits, and this is likely to raise the suspicion of Wendy. Instead, stego-cover *S* should “look” just like an innocent message even though it contains a hidden message.

Thus, it can be done [29] by Alice and Bob through equation (5), if $\alpha = \beta$ then P_e = 0.5 to operate on the 45° line in ROC plane as shown in Fig. 5. Alice can manipulate α and β values by employing an appropriate techniques or algorithms to force Wendy’s extractor tools to operate on the 45° line during a detection process (to be represented as *C = S = S’*). It means that the extraction tools will assume that the detection probability is equivalent to false alarm probability continuously.

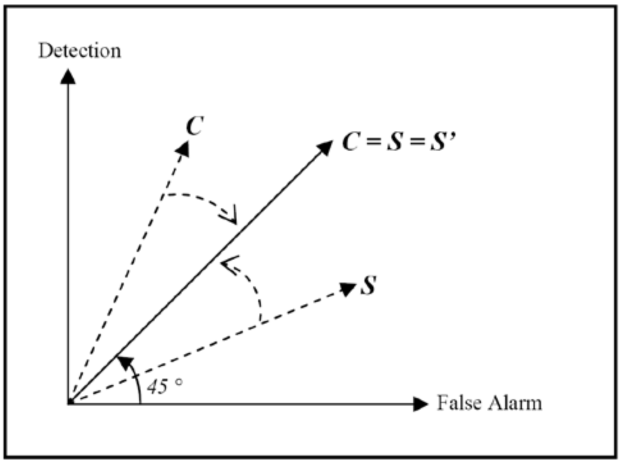


Fig. 5 A probability of steganalysis detection of steganography system

Therefore, Wendy does not have to clearly distinguish between the original stego message and stego-cover. It will make Wendy to assume that a stego message is an original stego message because she does not have sufficient information to make a decision based on this situation. However, there is a boundary of solution which the steganography system does not know on how competent the steganalysis detectors [30] on measuring the steganography system methods intelligently are. Thus, it seems like a hard challenge from Wendy’s point of view as a gatekeeper. It also raises an interesting question on deciding which is a *bestfit* method should be utilized in steganalytic system. As far as our knowledge is concerned, there is no standard method of steganalytic system has been used.

3 Conclusion

The primary contribution of this paper is to present the mathematical formulation works on steganalytic system. This paper also classifies and analyzes several conditional states of steganalytic system such as hypothesis testing, gaussion distribution, hidden markov model and vector analysis space. Through this work, it is assumed that a new approach on steganalytic system called *Intelligent Steganalytic System* (ISS) [31] will be produced in a near future. In particular, a further improvement is expected that computational intelligence techniques [32] such as neural network, genetic algorithm, and fuzzy logic will be manipulated and utilized in steganalytic system. This is because a fundamental goal of computational intelligence is the manipulation of human intelligence using the tools of computing science.

Acknowledgment:

This research work was fully supported by 1001/PKOMP/842025 of USM-RU-PRGS, Universiti Sains Malaysia (USM) and scholarship from Universiti Utara Malaysia (UUM) under the Higher Education Minister of Malaysia.

References:

[1] B. Deng, J. Tan, B. Yang and X. Li, A Novel Steganography Method Based on Modifying Quantized Spectrum Values of MPEG/Audio Layers III, *Proceedings of the 7th WSEAS Int. Conference on Applied Informatics and Communications*, Athens, Greece, August 24 – 26, 2007, pp. 325-330.

[2] R. Din, and H. S. Hussain, The Capability of Image In Hiding A Secret Message, *Proceedings of the 6th WSEAS International Conference on Signal, Speech and Image Processing (SSIP’06)*, Lisbon, Portugal, September 22 – 24, 2006. ISBN: 960-8457-53-X.

[3] C. Y. Chang, and S. Clark, Linguistic Steganography Using Automatically Generated Paraphrases, *The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics, Association for Computational Linguistics*, Los Angeles, California, June 2010, pp. 591 – 599.

[4] J. Fridrich, T. S. Holotyak and D. Soukal, Stochastic Approach to Secret Message Length Estimation in ±k Embedding Steganography, *Proc. EI SPIE*, San Jose, CA, January 16 - 20, 2005.

[5] H. Aboalsamh, H. Mathkour, S. Dokheekh, M. Mursi, and G. Assassa, An Improved Steganalysis Approach for Breaking the F5 Algorithm, *WSEAS Transactions on Computers*, Vol. 7, No. 9, 2008, pp. 1447 - 1456.

[6] M. Kharrazi, Performance Study of Common Image Steganography and Steganalysis Techniques, Special Section on Security, Steganography and Watermarking of Multimedia Contents, *Journal of Electronic Imaging*, Vol. 15(4), October - December 2006, 041104.

[7] G. Luo, X. Sun, L. Xiang and J. Huang, An Evaluation Scheme for Steganalysis-proof Ability of Steganalysis Algorithms, *International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (IIHMSP), Vol. 2, November 26-28, 2007, pp. 126 - 129.

[8] R. Chandramouli and S. K. Subbalakshmi, Current Trends in Steganalysis: A Critical Survey, *Control, Automation, Robotics and Vision Conference (ICARCV)*, Vol. 2, December 2004, pp. 964 – 967.

[9] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding for Steganography and Digital Watermarkin*g, Norwood: Artech House, 2000, pp. 56 – 92.

[10] K. Bailey and K. Curran, An Evaluation of Image-based Steganography Methods, *International Journal of Digital Evidence*, Vol. 2, No. 2, 2003.

[11] R. Chandramouli and N. Memon, Steganography Capacity: A Steganalyis Perspective, *Proc. SPIE Electronic Imaging 5022*, Santa Clara, CA, January 21 – 24, 2003.

[12] G. J. Simmons, Prison's Problem and the Subliminal Channel, *Advances in Cryptology: Proceeding of CRYPTO '83*, D. Chaum, ed. Plenum, New York, 1983, pp. 51 - 67.

[13] R. Din and A. Samsudin, A Conceptual Framework for Natural Language Steganalysis, *Proceeding of 2011 4th IEEE International Conference on Computer Science and Information Technology (IEEE ICCSIT2011)*, Chengdu, China, June 10 – 12, 2011, pp. 264 – 269, ISBN: 978-1-61284-833-4.

[14] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piottraschke, A. Westfeld, G. Wicke and G. Wolf, Modeling the Security of Steganographic System, *2nd Workshop on Information Hiding*, Portland, LNCS 1525, Springer-Verlag, April 1998, pp. 343 - 355.

[15] C. Cachin, An Information-theoretic Model for Steganography, *Proc. on the 2nd Workshop on Information Hiding*, Springer Lectures Notes in Computer Science, Vol. 1525, 1998, pp. 306 - 318.

[16] R. Chandramouli and N. D. Memon, A Distributed Detection Framework for Watermark Analysis, *ACM Multimedia Workshop on Multimedia and Security*, Los Angeles, CA, USA, November 2000.

[17] R. Chandramouli and N. Memon, Steganography Capacity: A Steganalyis Perspective, *Proc. SPIE Security and Watermarking of Multimedia Contents*, Santa Clara, CA, USA, January 2003.

[18] H. Poor, *An Introduction to Signal Detection and Estimation*, Springer-Verlag, 1994.

[19] S. Trivedi and R. Chandramouli, Active Steganalysis of Sequential Steganography, *SPIE Conference*, California, Vol. 5020, 2003, pp. 123 - 130.

[20] R. Chandramouli and K. P. Subbalakshmi, Active Steganalysis of Spread Spectrum Image Steganography, *IEEE Proceedings of the 2003 International Symposium on Circuits and Systems (ISCAS'03)*, Vol. 3, Issue, May 25 – 28, 2003, pp. 830 – 833.

[21] R. Chandramouli, A Mathematical Approach to Steganalysis, *SPIE Security and Watermarking of Multimedia Contents IV*, California, January 2002.

[22] D. Van Hieu and S. Nitsuwat, Image Preprocessing and Trajectory Feature Extraction based on Hidden Markov Models for Sign Language Recognition, *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD '08)*, August 6 – 8, 2008, pp. 501 – 506.

[23] P. Hervieu, P. Bouthemy and J. L. Cadre, A HMM-Based Method for Recognizing Dynamic Video Contents from Trajectories, *IEEE International Conference on Image Processing (ICIP)*, Vol. 4, 2007, pp. 533 - 536.

[24] B. Zhang, W. Dou and L. Chen, Audio Content-based Highlight Detection Using Adaptive Hidden Markov Model, *Sixth International Conference on Intelligent Systems Design and Applications (ISDA '06)*, Vol. 1, October 16 – 18, 2006, pp. 798 – 803.

[25] J. Li, K. Yue and W. Liu**,** An Adaptive Markov Model for Text Categorization, *3rd International Conference on Intelligent System and Knowledge Engineering (ISKE 2008)*, Vol. 1, November 17 – 19, 2008, pp. 802 – 807.

[26] N. F. Johnson, Z. Duric and S. Jajodia, *Information Hiding: Steganography and Watermarking – Attacks and Countermeasures*, Kluwer, USA, 2000.

[27] M. Sidorov, Hidden Markov Models and Steganalysis, *Proceedings of the 2004 Workshop on Multimedia and Security, ACM*, New York, September 2004, ISBN: 1-58113-854-7.

[28] N. Jiang, A Novel Analysis Method of Information Hiding, *Congress on Image and Signal Processing (CISP '08)*, Vol. 5, May 27 – 30, 2008, Sanya, China, pp. 621 - 625, ISBN: 978-0-7695-3119-9.

[29] R. Chandramouli, M. Kharrazi and N. Memon, Image Steganography and Steganalysis Concepts and Practice, *Lecture Notes in Computer Science*,

Springer Berlin/Heidelberg, Digital Watermarking, Vol. 2939, 2004, pp. 204 - 211, ISBN 978-3-540-21061-0.

[30] R. Anderson and A.P. Petitcolas, On the Limits of Steganograph, Special Issue on Privacy Protection, *IEEE Journal of Selected Areas in Communications*, Vol.16(4), May 1998, pp. 474 - 481, ISSN 0733-8716.

[31] R. Din and A. Samsudin, Intelligent Steganalytic System: Application on Natural Language Environment, *WSEAS Transaction on Systems and Control*, Vol. 4, Issue 8, August 2009, pp. 379 – 388, ISSN: 1991-8763.

[32] R. Din and A. Samsudin, Computational Intelligence in Steganalysis Environment, *Proceeding of the 7th WSEAS International Conference on Information Security and Privacy (ISP'08)*, Cairo, Egypt, December 29 – 31, 2008, pp. 48 – 53, ISBN: 978-960-474-048-2.