Steganography and Its Applications in Information Dessimilation on the Web Using Images as SecurityEmbeddment: A Wavelet Approach

Victor Onomza Waziri, PhD
Cyber Security Science Department,
School of Information and Communication Technology,
Federal University of Technology,
Minna-Nigeria
onomzavictor@gmail.com

Audu Isah, PhD
Department of Mathematics/ Statistics
Federal University of Technology,
Minna-Nigeria

Abraham Ochoche
Department of Information and Media Technology,
School of Information and Communication Technology,
Federal University of Technology,
Minna-Nigeria
abochoche@futminna.edu.ng

Shafi'i Muhammad Abulhamid
Cyber Security Science Department,
School of Information and Communication Technology,
Federal University of Technology, Minna-Nigeria
shafii.abdulhamid@futminna.edu.ng

Abstract— **This paper reviews the concept of Cryptography and Steganography and their differences are classified as a way of passing. The essence of steganography as an art of hiding information was examined using the wavelet approach. The algorithms developed and exhibited in block diagrams were experimentally examined with encrypted message and disseminated abstractedly over the Internet with the belief that the stego-image carrying the message would not be discovered by unauthenticated person.**

Keywords- Cryptography, Steganography, Steganalysis, Stego-Image, Wavelet, VoIP, steganogram, Communication Security, Secret Key Cryptography

I. .INTRODUCTION

Steganography is an ancient art of hiding vital information. This deceptive art encompasses various techniques of information hiding, the aim of which is to secret information into a carrier message. Steganographic methods are usually aimed at hiding the very existence of the communication. Due to the rise in popularity of IP telephony, together with the large volume of data and variety of protocols involved, it is currently attracting the attention of the research community as a perfect carrier for steganographic purposes.

*Corresponding Author: onomzavictor@gmail.com/

The purpose of steganography is to covert communication to hide messages from a third party. Steganography is the art and science of writing hidden messages in such a way that no

one apart from the intended recipient knows of the existence of the message [1].

In www.webopedia.com, steganography is also defined as the art and science of hiding information by embedding messages within seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files. This hidden information can be plaintext or ciphertext and even images.

Steganography differs from cryptography which is the art of secret writing, and is intended to make a message unreadable by a third party but does not hide the existence of the secret communication. Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography since hidden communication is a form of secret writing [2]. Nevertheless, this paper will focus on steganography as a separate field with application in despatching Security information over the Internet.

Steganography hides the covert message but not the fact that two parties are communicating with each other. The steganography process generally involves placing a hidden message in some transport medium, called the carrier. The secret message is embedded in the carrier to form the steganography medium. The use of a steganography key may be employed for encryption of the hidden message and/or for randomization in the steganography scheme.

IP telephony or Voice over IP (VoIP) for instance, is a real-time service which enables users to make phone calls through IP data networks. It is one of the most important services of IP-based networks and is impacting the entire telecommunications landscape.

An IP telephony connection consists of two phases in which certain types of traffic are exchanged between the calling parties: signalling and conversation phases. During the first phase certain signalling protocol messages, for example SIP (Session Initiation Protocol) messages [9], are exchanged between the caller and callee. These messages are intended to set up and negotiate the connection parameters between the calling parties. During the second phase, two audio streams are sent bi-directionally. RTP (Real-Time Transport Protocol) [1] is most often utilised for voice data transport and thus packets that carry the voice payload are called RTP packets. The consecutive RTP packets form an RTP stream.

Steganography is an ancient art that encompasses various information hiding techniques, whose aim is to embed a secret message (steganogram) into a carrier. Steganographic methods are aimed at hiding the very existence of the communication and therefore keep any third-party observers unaware of the presence of the steganographic exchange. Steganographic carriers have evolved through the ages and are related to the evolution of the methods of communication between people. Thus, it is not surprising that current telecommunication networks are a natural target for steganography and in particular, IP telephony is attracting the attention of the steganography research community. It is because of the following characteristics that IP telephony is a perfect carrier for steganographic purposes:

Being popular, its usage will not raise suspicions, which makes it to be considered as an anomaly itself.

The more frequent the presence and utilization of such carriers in networks, the better their masking capacity, as hidden communications can pass unnoticed amongst the bulk of exchanged data; potentially high steganographic bandwidth can be achieved. For example, during the conversation phase of a G.711-based call, each RTP packet carries 20 ms of voice; in this case, the RTP stream rate is 50 packets per second. Hence, even by simply hiding 1 bit in every RTP packet we can gain quite a high steganographic bandwidth of 50 bit/s.

Thus, many opportunities for hiding information arise from the different layers of the TCP/IP stack. Hidden communication can be enabled by employing steganographic methods applied to the users' voice that is carried inside the RTP packets' payload, by utilising so called well-known digital media steganography, or by utilising VoIP protocols as a steganographic carrier. It is a real-time service, which induces additional strict requirements for steganography detection (steganalysis) and simultaneously creates new opportunities for steganography (e.g. utilisation of excessively delayed packets that are discarded by the receiver without processing, because they cannot be considered for voice reconstruction).

Presently, steganographic methods that can be utilised in telecommunication networks are jointly described by the term network steganography or, specifically when applied to IP telephony, by the terms VoIP steganography or steganophony [4]. These terms pertain to the techniques of hiding information in any layer of the TCP/IP protocol stack, including techniques applied to the speech codecs, or those that utilise the speech itself.

In general, steganography can be treated as a double-edged sword depending on who uses it and how. However, the ethical issues related to the utilisation of information hiding techniques require consideration in a broader steganography context, which is beyond the scope of this paper. The main application of network steganography is for providing a means of conducting clandestine communication. The purposes for establishing hidden communication can be varied; possible uses can fall into the category of legal or illicit activities. The illegal aspect of steganography starts from criminal communication, through confidential data infiltration from guarded systems, cyber weapon exchange and control, up to industrial espionage. Legitimate uses include circumvention of web censorship and surveillance, computer/network forensics, or copyright protection. Techniques can be used with VoIP to improve its resistance to packet losses and improve voice quality [1], [5], extend communication bandwidth [6] or provide means for secure cryptographic key distribution [7] via images.

The expansion of TCP/IP networks opened up many possibilities for covert communication due to changes in the traditional circuit-switched networks paradigm; services/applications are created by the network users rather than by the network itself, the transport and control functions are not separated and can be influenced by the user. These possibilities are a consequence of the fact that network users can influence, and/or use the control of data flow – the communication protocols – together with the service/application functionality of terminals to establish covert communication. That is why secret messages can be hidden, not only within ordinary non-covert (overt) messages as in traditional steganography and circuit-switched networks, but also in the communication protocol's control elements, in effect by manipulation of the protocol's logic, or by combinations of the above.

Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so that it cannot be understood; the Steganography hides the message so that it cannot be seen. In this paper, we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and Security. Presently, we have very secure methods for both cryptography and Steganography – AES algorithm is a very secure technique for cryptography and the Steganography methods, which uses frequency domain, are highly secured. Even if we combine these techniques straight

forwardly, there is a chance that the intruder may detect the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding. This paper mainly focuses developing a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography and have them hidden in an image. As we know that-

Hiding data is better than moving it shown and encrypted. As we now know, cryptography and steganography have been known for many years. We can encrypt data, but it will be exposed while transferring. On the other hand, we can hide data into a common object, but if someone extracts it, he/she can get the information easily. Therefore, our idea is to apply both of them, so in case one gets the embedded stuff; she/he will face an encrypted data.

There are important connections between steganography and cryptography but both have very different goals. The goal

Nonetheless, still there is a chance that the intruder can break the code. In our new system instead of applying existing techniques directly, we will be using the following approach –

Instead of hiding the complete encrypted text into an image, we will be hiding a part of the encrypted message.

Unhidden part of the encrypted message will be converted into two secret keys.

In this system to get the original message one should know, along with keys for Cryptography and Steganography, two extra keys and the reverse process of the key generation. So our final goal of the project is to develop a new system which is highly secured and even if somebody retrieves the message from stego image [2] it becomes a meaningless for any existing cryptographic techniques.

The rest of the paper is arranged as follow: Section 2 gives a brief related literature review. Section 3 dwells more in details on the concepts of Steganograhpy and Cryptography.

II. BASIC CONCEPTS AND RELATED WORK

There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements [3] for cryptography, including Authentication, Privacy/ Confidentiality, and Integrity /Non-repudiation. The three types of algorithms are described:

(i) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption

(ii)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

(iii) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information. Steganography is the of steganography is to keep the existence of a message hidden or to hide the fact that communication is taking place. In contrast, the goal of cryptography is to obscure a message or communication so that it cannot be understood. With this in mind, the security ability of both techniques is also different. In cryptography, the message is not hidden therefore a hacker can try to intercept and decrypt the message but with steganography, the hacker must discover the medium before he/she can try to intercept it. Putting their differences aside, steganography and cryptography make great partners. It is very common to use these techniques together. As an additional security measure, a steganographer can encrypt the message before it is hidden using steganography techniques. We must note this matter of facts:

To hide data in a popular object that will not attract any attention.

In case the data is extracted, it will be encrypted.

other technique for secured communication. It encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images [5], audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers

[6] used (graphics, sound, text, executables) or by the techniques used to modify the covers

a) Substitution system [7,22].

b) Transform domain techniques [8]

c) Spread spectrum techniques [10,20]

d) Statistical method[11]

e) Distortion techniques [12]

f) Cover generation methods [12]

III. STEGANOGRAPHY AND STEGANALYSIS

Today, networks are in perpetual state of being seriously threatened by web hackers using different intruding devices. Cryptography can be used at different levels of TCP/IP security levels using different computational models. As earlier emphasized, steganography is the art and science of hiding information by embedding messages within others, seemingly in an innocuous and indevastating channelling of peaceful message on transaction. In Greek, steganography means ‘cover writing’. Steganography is the direct opposite of cryptography in a sense that the information being channelled is hidden while cryptography bits are exposed with gibberish exposures. The main goal of steganography is to hide information from the man-in-the-middle view. A famous illustration of steganography is Simmons’ problem as referenced in [13-14]. An assumption that can be made from this problem is that once the sender and the receiver share some basic secret information

in form of code, then the corresponding codessteganography protocol becomes the secrete key. Pure steganography means that there is no prior information shared by the sender and receiver. If the public key of the receiver is known to the sender, then the protocol is known as the public key steganography [14-15] protocol. Almost all digital files formats can be used for steganography, but image and audio files are more suitable because of their high degree of noises or redundancy [15]. Digital file formats can be used for steganography, but the formats that are most suitable are those with high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy for greater than necessary for the object's use and display [13]. The redundant bits are detected easily [14]. An obvious method was to hide a secret message in every nth letter of every world of a text message. Digital representation of image has a large amount of redundant bits and for that images are the most popular cover objects for steganography.

A. Steganography as a Phenomenon of Information Hiding in Images

Many methods abound in which Images are significantly used to hide secret information; of the algorithms is the wavelet transforms [17]. The technicality for the computational procedures for this algorithm is mathematically intractable and the reader may be willing to read any mathematical analysis in text based on the Fundamentals of Multimedia for more details. Nonetheless, many applications use the wavelet decomposition taken as a whole. The common goals concern the signal or image clearance and simplification, which are parts of de-noising or compression. There are many published papers [18-19] in oceanography and earth studies on wavelet. One of the most popular successes of the wavelets is the compression of FBI fingerprints.

When trying to classify the applications by domain, it is almost impossible to sum up several thousand papers written within the last 15 years. Moreover, it is difficult to get information on real-world industrial applications from companies. They understandably protect their own information.

In mathematics[17], a wavelet series is a representation of a square-integrable real number or complex number or complex valued function by a certain orthornormal series generated by a wavelet.

A function $\psi \in L^2(R)$ is called an orthonormal wavelet if it can be used to define a Hilbert basis, that is a complete space or complete orthonormal system [16], for the Hilbert space L2(R) of square integrable functions.

The Hilbert basis is constructed as the family of functions $\psi_{i.k}(x) = 2^{\frac{i}{2}}\psi(2/x-k)$ by [15] means of Dyadic transformation or dyadictranslations and dilations of ψ is $\psi_{i.k}(x) = 2^{\frac{i}{2}}\psi(2/x-k)$ for integers $j,k \in Z$. This family is an orthonormal system if it is orthonormal under the inner product $(\psi_{jk},\psi_{lm})\frac{\delta_{ji}}{\delta_{kn}}$ where δ_{ji} is the Kronecker delta and (f, g) is the standard inner product

$$\int_{-\infty}^{\infty} f(x)g(x)dx \in L^2(R)$$

The requirement of completeness is that every function f∈ L2(R) may be expanded in the basis as

$$f(x) = -\sum_{j,k}^{\infty} C_{i,j}\psi_{i.j}k(x)$$

The integral wavelet transform is defined as

$$[W\psi f] = \frac{1}{\sqrt{|a|}}\int_{-\infty}^{\infty}\psi(\frac{a-b}{a})f(x)dx$$

The wavelet coefficients cjk are then given as

$$C_{jk}[W\psi f] = (2^{-j}, k2^{-j})$$

where

$$a = 2^{-j}$$

is called the binary dilation or dyalic dilation and $b = k2^{-J}$

is the binary or dyalic position.

Wavelet analysis is capable of revealing aspects of data that other signal analysis techniques cannot, aspects like trends, breakdown points, discontinuities in higher derivatives, and self-similarity.

Furthermore, because it affords a different view of data than those presented by traditional techniques, wavelet analysis can often compress or de-noise a signal without appreciable degradation. Indeed, in their brief history within the signal processing field, wavelets have already proven themselves to be an indispensable addition to the analyst's collection of tools and continue to enjoy a burgeoning popularity today. For want of space, any researcher wanting to have a clear understanding of the algorithms should consider reading Fourier transform, Continuous Wavelet transform and the Discrete Wavelet Transform.

In the JPEG compression standard, images are transformed successively into 8x8 block pixels. Each pixel block is passed through a 2-dimensional DCT to produce 64 DCT coefficients for each block. The DCT coefficients F(u,v) of an 8 x 8 block of image pixels f(x, y) are illustrated below;

$$F(u,v) = \frac{1}{4}(u)C(v)\sum_{y=0}^{7} f(x,y)(\cos\frac{(2x+1)u\pi}{16} + \cos\frac{(2x+1)v\pi}{16}$$

where $C9x) = 1/\sqrt{2}$ when x equal 0 and $C(x) = 1$.

$$F^{Q}(u,v) = \frac{F(u,v)}{Q(u,v)}$$

Where $Q(u, v)$ is a 64-element quantization table.

The Least Significance Bits (LSBs) of the quantized DCT coefficients can be used as redundant bits in embedding the hidden messages. Modification of any single DCT coefficient affects all the 64 image pixels.

Wavelet transform is growing up rapidly. Wavelets have been effectively utilized as a powerful tool in many diverse fields including approximation theory; astronomy, physics, signal processing and image processing etc.

Many practical tests propose to make use of the wavelet transform for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the information hiding system features.

The hierarchical nature of the wavelet representation allows multi-resolutional detection of random vector added to all the high pass bands in the wavelet domain. It is demonstrated that the subject to distortion from compression, the corresponding hidden message can be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain.

B. Steganography Techniques

This paper considers two algorithms based on Image Domain Techniques and Image algorithms for wavelets techniques.

B.1 Image Domain Technique

Denoting x at an instance of a class of potential cover media, such as JPEG compressed images transmitted via the (cloud) internet, for instance. If we treat x as an instance of a random variable X, considering the probability distribution $P(x)$ over transmissions of this class of media. Thus, transmitting signals drawn from $P(x)$, it can be assured that they are indistinguishable from similar transmissions of the same class regardless of how many such signals transmitted. Since $P(x)$ represents data taken from the real world, a valid instance of $P(x)$ can be drawn using a digital recording devices. Given such a sample x, we separate x into distinct parts, xa which remains unperturbed, and xb which will be replaced with x'b the encoded message. For LSB encoding, xa represents the most significant bit of the cover coefficient as weak as any coefficients not selected to coefficients. Considering these parts as two dependent random variables xa and xb. By the model distribution Px, the estimate of the distribution over possible values of xb conditioned on the current value for xa

$$P(xb/bx(xa/bx)) = ax$$

provides the selected xa so as to obey this conditional distribution, the resulting $x' = (ax, bx)$) will be correctly distributed according to model $P(x)$.

Since $P(xa/bx)$ cannot be modelled perfectly; but $P(x)$ can be perfectly modelled. While the human visual system is fantastic at modelling images, it lacks certain degree of precision. This lack of precision is what LSB encoding methods exploits. However, even the simplest models, such as that captured the marginal statistics of xb, do not lack this precision, and thus can be used to detect when LSBs are modified by some other distribution.

The below figure 3.1 illustrates a proposed model based on steganography for encoding steganography. First, an instance x of the class of cover media X is separated into xa and xb. xa is fed to the model estimate of $P(x)$ which is used to compute the conditional probability distribution $P(xa/bx)$. The compressed and encrypted message M is given to an entropy decoder which uses $P(xa/bx)$ to decompress M resulting in a simple drawn from the distribution. The parts xa and xb are then combined to form the steganogram x', distributed according to the model $P(x)$ which is transmitted to the receiver.

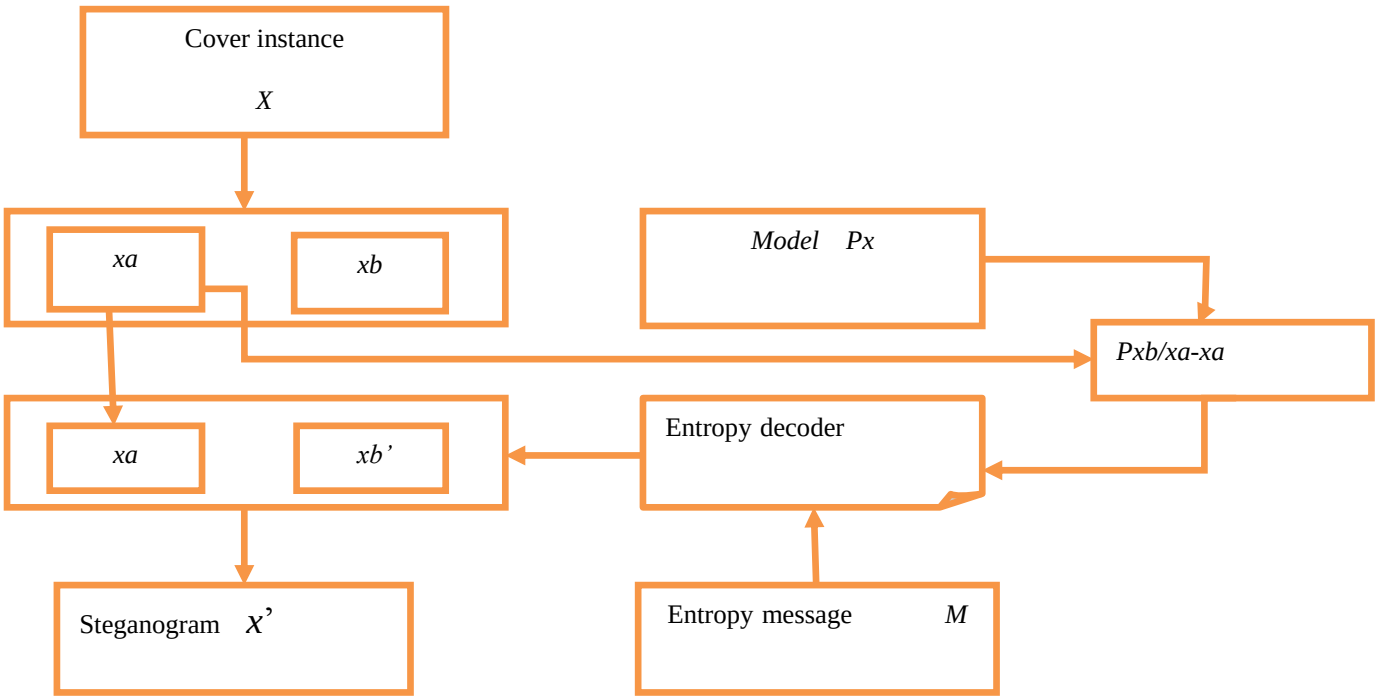
The below diagram in figure 3.2 illustrates the method used to recover the original message. The steganogram x' is divided into $xa\ and\ x'b$. The xa portion is fed into the model $P(x)$ which is again used to compute the conditional distribution $P(xa/bx)$. The same model is given entropy encoder that was fed into the entropy encoder during the encoding stage.

C. Capacity

The capacity determination of how a message can be hidden inside a cover message without becoming detectable had been a long unanswered question $P(x)$. The of Modelling $P(x)$ perfectly to ensure total security of the cloud by estimating the average maximum message length that can be hidden without becoming detectable by the measured statistics of $P(x)$. hat xa is being used as an information channel, as

in information theory that states that the amount of information on average that can be transmitted through such a channel is equal to the entropy of the conditional distribution $P(xa/bx)$. By the model, capacity limit can be measured for

$$H(xb/xa) = \sum_{xb} \frac{pxb}{xa(\frac{xb}{xa})} \log_2 pxb/xa(\frac{xb}{xa})$$



a given xa which is the usual classical entropy equation

Figure 3.1: Encoding Stego-Image

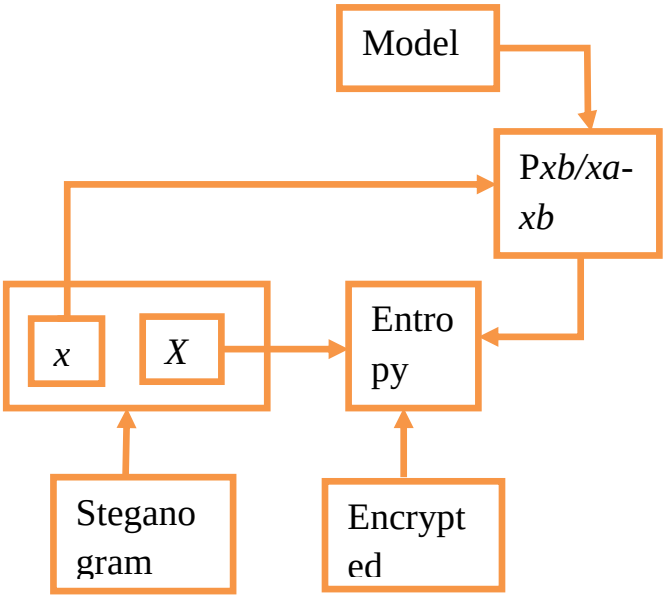


Fig. 3.2: A model based steganography decoder

D. The Embedded Message Model

The model is fit into the histogram for an image to compute the probability of each offset symbol for a coefficient given in binary index. The offset symbols and probabilities are passed to a non-adaptive arithmetic entropy decoder [23] along with the message wished to embed in the cover image. The offset symbols returned by the entropy decoder comprise x'b which are combined with the bin indices to compute the coefficient values of the histogram x'. Permutative Straddling[25] a technique used for computing pseudo-random permutation seeded by a key as order in which the coefficient are used in encoding messages. Running out of symbol probabilities before running out of bits, means that the message maximum message length of the image is reached, maximum length is obtained by computing the entropy of the symbol frequency. For shorter messages of maximum length, the remaining symbols are assigned according to the original coefficient offsets so that these coefficients remain unchanged.

D.1 Embedding Efficiency

The way of demonstrating the effectiveness of the model approach is by calculating its embedding efficiency. This is the average number of message bits embedded per change of the coefficients [21]. The assumption is that the more changes

made to the coefficients, the easier on average it will be to detect the steganography, thus minimizing the number of these changes for a particular message length. In the model based approach, the embedded efficiency will be determined by the entropy of the symbol distributions. [24] Taking embedding size 2 which corresponds to LSB encoding hence each non-zero AC coefficient can be taken to two new values, hence comparing with other steganography methods by achieving an embedding efficiency greater than or equal to 2, regardless of the message length.

Where k represents the probability coefficient of one of the two offset symbols for a given coefficient in a given embedding efficiency function

The average number of bits encoded or the embedding rate is equal to the entropy of the channel as;

$$H = (k \log_2 k + (I - K) \log_2 (I - K)$$

The Probability that the value of the coefficient will be changed by encoding a different symbol that the original one, the rate of change is;

$$k(I - k) + (I - k) = 2k(I - k)$$

The expected embedding efficiency is the ratio of the above as:

$$[efficiency\ ] = \frac{(k \log_2 k + (1-k)\log(1-k))}{2k(1-k)}$$

Which is never smaller than 2 for $0 < k < 1.$. If $k = \frac{1}{2}$, the embedding efficiency will be exactly 2 reasons, by encoding the message at a rate of 1 bit per coefficient and changing a coefficient from its original state half of the time. Otherwise the embedding efficiency will be greater than 2 becomes the largest (and the smaller capacity) when the symbol probabilities are far apart. The F5 algorithm uses a matrix encoding to obtain an arbitrarily high embedding efficiency by reducing the message capacity as discussed in the previous section. However, for its maximum message capacity which is around 13%, the embedding efficiency is only 1.5 [21]. The OutGuess algorithm, since it the most changing about two coefficients on average for every other bit it embeds, it has an embedding efficiency of close to 1. In practice it is found that OutGuess provides an embedding efficiency of 0.96 and a maximum message capacity of about 6.5%

IV. EXPERIMENT

This section examines the results of the test run by the new steganography technique designed for implementation for this paper. During the implementation phase, the researchers tested the algorithm for different sets of images as well as text documents. For each and every normal JPG images for the proposed technique the messages is first encrypted and then embed in the JPG image.

A. The Model for the Information Hiding

The message is the composition of some character. Every character of the message can be represented as an ASCII value which is either even or odd. Depending on this evenness, the character is encrypted differently and then steganographed for onward transmission to the recipient without being suspected by the man-on-the middle-the eavesdropper .

A.1 Discussion and Summary of Results

Figure4.1: Cover image

Figure4.2: Stego-image

From the steganographic presentation above, the cover image and the stego-image cannot be different from each other. The resolution and size of both remain the same. The text document embedded in the cover image that produced the stego-image is here displayed below;

The Boko Haram (BH) sects are becoming stronger every day. A close friend informed me that they are recruiting non-Muslim faithfuls who are cyber security experts especially in Staganography for a contract of two million US Dollars for just four months. That much allowance of another three million Dollars available for those who can bring down some big companies and Government big functionaries such as the NNPC refineries and PHCN computer functionalities through hacking. They are more aggrieved with the PHCN because of its failure to supply constant light. Hence, they have taken the battle electronically. You had once told me of your interest in joining the sect should any big offer is given; and as a guru like your shrewdness in software engineering should meet their

desire); I think of informing you that you may join the quick money spindling at the mercy of innocent souls. With your experience in software development, there is some money allocated to it especially for the development of steganography algorithms. The cost for the software development is five hundred thousand Dollars. Should you be interested, do not hesitate to make cold money from BH since government is negligent to the common man's plight. This is a top secret review of the current BH development. Read more details from www.bokaharam.org.ng Top Secret and remains top; divulge this information to the police at your peril.

Text document is encrypted to the gibberish below which is the result of the encrypted text document before embedding into the cover image is displayed below:

Kk02bgDMADAAzQAaIEYAfwBvAK4AWABPAC4ALQA
zAP8ACwASABkgBAAdIGYACAAJANcAtQCNAC0AawA
LAH4BZwAfAFAAxwBKAGcAYgC2AOgA/QBLAPkAQg
BsABYABADwALEABgBTAVIBrgD5AFQAVgDaAI8Azg
AdAF8AxABvABkgRwCoACUAswDJAFkAwQAaIEAAjw
AUILQAHw`B3AHwAuQD4AF8A3AIJAA8AZQBjAKoAIg
BAADoAbgA/ABEAvgDpAKcA8AAjAHQAdgC9APEAwQ
A3AGwA+wAXAN8ACgAIAAMAtAC2AGgAISCpAEsAsg
C1AHEA5wDgABAAoABZAKwgHgDwAMYCbAAwIPcA
MgBHAAQA+ABSAVIB2wCvAFMArgAmABMgOiDYAN
oAdQBeAAwAIwA5AGQAcAAXAFoA2wAWAB0g4wC2A
D4AQABRACMA0ADcAEcAwgBgAB4ArAC1ABgg9gD6A
LUAIgAOAPoA3AILAOwAOgCdADQAGAAHAKwgICBB
AKsABwA9AEcAMQDxADAAQgDvADkA9gABAPsAXgB
nAFIAQwA8AFsAoAC6AIEAYgD+APQAuAATAEkAXQB
rAOIAPgC/AD0AkABGAB8A1ACmALkAVwAyAAYAyQ
CsIGoAygDJAHgBGADkAHsAwwAuADwAKwBaAK4Ay
QAZIGAB9gAcAKwg3wDQAOgAuwAlACAgJgDyAMcAc
wCkAOQAfgAiIA8AeAHKAEIAqQC4AH4AbABiAA8AGi
BaACEg0QAWAFIAHgA+ABkgWABUAP0AygBbAEYAZ
wBDAF0AIAD8ABsAowAcICAAPgBSAQ4AZgBuAAMAB
wAfAAAAxQBgAWEBDwCqAEQAOSAEAC8ANADyAD
4ApwBWACsARAC4AOIAcQDYAF8AsAAiIHUATQAEA
EIACgAVADEALwAaIPcAtQDbAGoAEwDpAFoAPACrA
DAA2ACuAOEA/AAoAFAAJgBUAH8AwQBjAO4AHwBh
ATAg7gBSACYAGSDlACsAzABMADMAdQBmAKcADg
C5AOYA1gCjAFwA0gB0AKYAQwBkADog/wDEADAA2
AB7ADkgISAiIBwgfgFKABcAygBTAacAEgATIAwAeAFz
ABggXwB9ARog+AA5ALkASwAHAHgAEgDQAH4BFQA
VAK8A0AB9AMkAEwAOAC8AZgDbABkgFgCdAKAA6g
C/ABMgKwC8AB0gbAD3ANgAKQCsIBUALAAkAFoAaw
CQALkAfADTAHYAKgBVAGABogBnAA0AugDWACAg
0AD4ANgAjwDSAH4B8wBWANIAAgCsIFcA7QBDAMw
AVAC9AFQA+AA6IAEAgQDeABUAHSAOAMcArwBaAP
IA/wC6AFIAGQALANoA+gC2AOYABAA6AHcAnQBeAP
8ASQBFAEcAwgAbABUAeACsAI8A0gDJABUAeAHSAK
wAtgDMABYA4wB9AW8AqQBSAcQA6wByAKMAFCBN
AM8AEyDFABwAUgFhABogQQCQAA0ADgC+AO8AOA
C1ACUA8ABaANEA7wBTAbMAUAAsAH4BFQD8AMcA
UwHLADgApgCwAHIAtQCoAE0AKQDoAPQA6AD/AKs
AIADoAEYAGgAiINYAVgA4ACAAGSD+ALIAIQAlAMs
AQwDGAnUAOwCqAE8ArCAaANYAwQCkALgAxgJDAF
sATwDzAE0AxQDLAGsAuAABAL4A1gDdAAMAGgDrA
NYAKABYALQAtgDEAKwgcAC1APkAPABhAKIAISAIA
D0AfQB3AN0AkAD4AMQA0gB+ACcAEgAJAKcApQC+A
NoAWABLADYAGSCwAM8AYQByABEAWQBEADIAIi
DXAGEAfAAkAEYA8ABJABoAtAAiIP8AwgAgABgg/QB
aAMsAJgA0AG8AGQAwILsA2gB1AHkAISDQAOUAQgA
+AKwAXQDeAHAAKQAKAMQAfQGxANwCvQCdAOsA
dgDyADcAxQBRAH0AAAB2AKUAxQDCAPwAfgFAAFQ
AaQDbAGwA2QC7AMkAPABeAHIADwDBANIALwBJA
O0AIABVANoAOwD2APEASAAYIOkAvAA5IDAANQAw
ABwAMQBLAGABjQA0ADAADgB1AOIAfAD0AAUAsg
BsAPAAEgAnAEUArQCtABEAwADcALIAtwA9AEkAáFF
339C511FE17CEA11B7FF1000B6BAABékK

The resultant encrypted text document before embedding into the cover image becomes the stego-image. This idea achieves dual targets for security attempts breakage. In the first place, the message is encrypted and later hidden in an image as shown in figures 4.1 and 4.2. Figure 4.1 depicts the cover Image while Figure 4.2 hides the stego to all view in the same image now christened stego-image. Should any persons intercept figure 4.2, when opened, such a one would meet the difficulty of encryption.

V. CONCLUSION

For designing the steganography application, the researchers worked on different phases like the embedding/encrypting, extracting/decrypting and data transmission. An application for sending the personal data securely to the destination (receiver) was developed successfully.

The design is the primary phase which gives a brief idea about the different levels used for developing an application with the help of block diagram and the result shown above. The most important phase in the research is the execution phase. For executing the application, the researcher worked on two sections; one is the embedding/encryption and another is the extracting and decryption. The researcher had issues in deciding for a program to encrypt the text documents and embed same into the cover image to get the resultant stego-image and transmit same over the Internet. After much, software was reached to encrypt the text document and embed the text. Different approaches were reached in testing the application and several cover images with different text documents were sampled.

Concentration was centred on encryption on text documents and embedding same in cover image to produce a stego-image. Normally after embedding the data into the cover image, the stego-image may loss its resolution. In the proposed approach, the image remains unchanged in its resolution as well as size as could be seen in the cover image and the stego-image above. The speed of embedding the data into the cover image is also considerably high in the proposed technique such that the

stego-image is protected and the data is sent to the destination securely.

For the extraction and decryption phase, the software was able to reverse the plain text document and retain the cover image after applying the secret key. Security key like personal password for protecting the image from unauthorized modification is used to improve the security of the cloud computing.

The final phase which is the transmission of the data to the destination (from sender to receiver). The researcher made use of key section for protecting the data from unauthorized modification while the stego-image is in transit. The application uses the password as the reference such that whenever the image is sent using web sources like the e-mails to the destination.

REFERENCE

[1]. Wikipedia. http://www.wikipedia.com/ 2006
[2]. Bauer, F. L. *Decrypted Secrets: Methods and Maxims of Cryptology*, 3rd ed. Springer-Verlag, New York, 2002.
[3]. Cole, E. Hiding in Plain Sight. Wiley, John & Sons, Incorporated. 2005
[4]. Arnold, M., Schmucker, M., and Wolthusen, S. D. *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House, Norwood, Massachusetts, 2003.
[5]. Artz, D. Digital Steganography: Hiding data within data. *IEEE Internet Computing* (2001) 5(3):75-80.
[6]. Farid, H. Detecting Steganographic Messages in Digital Images. Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001.
[7]. Fridrich, J. and Goljan, M. Practical steganalysis of digital images: State of the art. In: *Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV*, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 1-13
[8]. Callinan, J. and Kemick, D. Detecting steganographic content in images found on the Internet. Department of Business Management, University of Pittsburgh at Bradford [Online]. (December 11, 2003)
[9]. Warcking:Warcking; Collaboratively Creating a Hobo-Language for Wireless Network (online) 2003
[10]. Stefan K.,;Fabian A. P. P: Information Hiding Techiques for Steganography and Digital Watermarking. Artech House Boston SSBN 1-58053-035-4, pages 237
[11]. Hosme,r C. and Hyde C.; 'Discover Cover Digital Evidence' Digital Forensic Research Workshop (DFRW) 2003
[12]. Kennard , S. and Mark, C. SAMS; 'Understand Soap', the Authorities Solution, SAMS Publishing 2000.
[13]. SOAP Security; http://www.w3.org/TR/SOAP-dsig/
[14]. S. Inoue, K. Makino e tal; A proposal on Information Hiding Method Using XML. http://takizawa.gr.jp/lap/nlp-xl
[15]. Mell, P., Grance, T., NIST definition of Cloud Computing; National Institute of Standard and Technology, 2009.
[16]. Amazon definition; http://amazom.com/ 2008
[17]. Stegagonagraphy; Official Courseware ; Computer Hacking Forensic Investigator [312 – 49] EC-COUNCIL. http://www.eccouncil.org/
[18]. Pettitcos F.; MP3 Stego 1998
[19]. Provos N.; 'Detecting Against Statistical Steganalysis .' In Proc. 10th UNSENIX Security Symposium. Washington DC 2001
[20]. Westfeld, A. and Pfitzmann, A.: Attacks on Steganographic Systems. In: Pfitzmann A. (eds.): 3rd International Workshop. Lecture Notes in Computer Science, Vol.1768. Springer-Verlag, Berlin Heidelberg New York (2000) 61−75
[21]. Westfeld, A.: High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm). In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, Vol.2137. Springer-Verlag, Berlin Heidelberg New York (2001) 289– 302
[22]. Cole, E. Hiding in Plain Sight. Wiley, John & Sons, Incorporated. 2005.
[23]. Van, H. J., 'Introduction to Coding Theory' 2nd Springer-Verlag 1992
[24]. Fridrich, J., Goljam, M., and Hogea, D., 'Steganalysis of JPEG Images; Breaking the F5 Algorithm', Proc. 5th Intl Workshop Information Hiding, Springer-Verlag, 2002
[25]. Steganography software for Windows, http://members.tripod.com/steganography/stego/ software.html 2002.