IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 2, Issue 5 (July-Aug. 2012), PP 01-15
www.iosrjournals.org

Mathematical Modeling of Image Steganographic System

Kaustubh Choudhary
Scientist, Defence Research and Development Organisation (DRDO), Naval College of Engineering, Indian Naval Ship Shivaji,Lonavla, Maharashtra, India

Abstract: *Image based steganography is a dangerous technique of hiding secret messages in the image in such a way that no one apart from the sender and intended recipient suspects the existence of the message. It is based on invisible communication and this technique strives to hide the very presence of the message itself from the observer. As a result it becomes the most preferred tool to be used by Intelligence Agencies, Terrorist Networks and criminal organizations for securely broadcasting, dead-dropping and communicating information over the internet by hiding secret information in the images. In this paper a mathematical model is designed for representing any such image based steganographic system. This mathematical model of any stego system can be used for determining vulnerabilities in the stego system as well as for steganalysing the stego images using same vulnerabilities. Based on these mathematical foundations three steganographic systems are evaluated for their strengths and vulnerabilities using MATLAB ©Image Processing Tool Box.*

Key Words: *Cyber Crime, Global Terrorism, Image Steganography, LSB Insertion, Mathematical Model of Image Steganographic System*

I. Introduction

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient suspects the existence of the message. It is based on invisible communication and this technique strives to hide the very presence of the message itself from the observer. Herodotus's Histories describes the earliest type of stegenography. It states that *"The slave's head was shaved and then a Tattoo was inscribed on the scalp. When the slave's hair had grown back over the hidden tattoo, the slave was sent to the receiver. The recipient once again shaved the slave's head and retrieved the message".*

All steganographic techniques use Cover-Object and the Stego-Object. Cover-object refers to the object used as the carrier to embed the messages into it. In the above example the slave's head (without tattoo) is the cover object. In modern context Images, file systems, audio, video, HTML pages, word documents and even email-spams can be used as cover objects. Whereas stego-object is the one which is carrying the hidden message. I.e. in the above example the '*slaves head with fully grown hair and a hidden tattoo*' is acting as the stego-object. Contemporary Steganography can be of various types depending upon the nature of the cover object and the method used for hiding information in that cover object. This technique is frequently used in espionage, organized crime and is especially popular among terrorist networks.

Among all those steganographic techniques the digital Image based steganography is most commonly used due to numerous advantages offered by it.[1] But the most important advantage is substantial difficulty in steganlysis of the digital image. Steganalysis is the process of identifying stego-objects from the bulk of innocent objects and further extracting the hidden information from the same. The identification of the steganographic signature in the innocent looking stego-image is the most difficult part of any steganalysis algorithm. Once this malicious stego-image is identified then either the hidden data can be extracted from it or the data in it can be destroyed or can be even used for embedding counter-information in the same

Digital image consists of numerous discrete pixels. Any pixel P(x,y) located at x^{th} row and y^{th} column of the image has a particular color which is combination of the intensity levels of three primary colours Red, Green and Blue and jointly called as RGB value of the pixel P(x,y). For example in a 24 bit BMP image RGB values consists of three 8 bits for each R,G and B and thus a pixel is a combination of 256 different shades (ranging from intensity level of 0 to 255) of red, green and blue resulting in 256 x 256 x 256 or more than 16million colors. Thus if the least significant bits in the R, G and B value are changed the pixel will have minimal degradation of 2/256 or 0.78125%.This minor degradation is psycho-visually imperceptible to us due to limitations in Human Visual System (HVS). But at the cost of this negligible degradation 3 bits (1 bits each from red, green and blue) are extracted out of every pixel for transmitting our secret information. The most of the Spatial Domain Image steganographic techniques use this method of LSB Insertion for hiding data in the image. There are other techniques also for hiding data in the image. For example Transformation Domain Steganography may use Discrete Cosine Transforms or Discrete Wavelet Transform for embedding data and some other steganographic algorithm may use a different color space itself (Example RGB may be converted to YCbCr and then various steganographic techniques can applied).

In this paper a Universal mathematical model is designed for representing any Image Based Steganographic System unambiguously as a mathematical structure. Based on this mathematical model three Spatial Domain Transformation based LSB Insertion algorithms are evaluated for susceptibility to steganalysis.

II. Mathematical Model of Image Steganography System

Any steganographic algorithm or simply Stego-algorithm is composed of Stego-Function □ and inverse of Stego-Function □$^{-1}$. □ takes Cover-Image C and Information I as input and generates Stego-Image S as the output. At the receiver end the Stego-Image S is fed to decoding algorithm which is mathematically inverse of Stego-Function □ (represented as □$^{-1}$) and produces Information I. These two function along with the entire set of their domain and co-domain form the Steganographic System Ψ (or simply Stego-system). Mathematically this can be represented as S = □ (C, I) and I = □$^{-1}$(S) and Ψ = {□, □$^{-1}$$_{,}$ C, S, I}.

2.1 Universal Stego System: A perfect Depicter of a Stego-Algorithm

A same stego-algorithm may operate on different cover images and may insert different informations in them. So any stego system Ψ = {□ , □$^{-1}$$_{,}$ C, S, I} is different for every pair of cover image C and Information I even though the Algorithm of Stego- system Ψ given as Ψ(Algorithm) = { □ , □$^{-1}$} remains the same for all those pairs. So we introduce the concept of Universal Stego System which is Universal Set of all stego systems Ψ = {□ , □$^{-1}$$_{,}$ C, S, I} which have same Stego-Algorithm Ψ(Algorithm) = { □ , □$^{-1}$}.We represent any Universal Stego System by Φ ={ □ , □$^{-1}$$_{,}$ ℂ , 𝕊, 𝕀 } where ℂ is set of all cover Images, 𝕊 is set of all stego-images and 𝕀 is set of all Information and stego algorithm of Φ given as Φ(Algorithm) = { □ , □$^{-1}$}. Thus any stego system Ψ = {□ , □$^{-1}$$_{,}$ C, S, I} is an instance of stego algorithm { □ , □$^{-1}$} or Universal Stego System Φ ={□ , □$^{-1}$$_{,}$ ℂ , 𝕊, 𝕀 }.
Mathematically we represent a Universal Stego System Φ as:

$$
\begin{aligned}
&\Phi = \{ F, F^{-1}, \mathbb{C}, \mathbb{S}, \mathbb{I} \} \\
&\quad = \{x : x \text{ is stego-system } \Psi \text{ with } \Psi(\text{Algorithm}) = \{ F, F^{-1}\} \} \\
&\text{Stego-algorithm of } \Phi \text{ or } \Phi(\text{Algorithm}) - \{ F, F^{-1}\} \\
&\mathbb{C} = \{C: C \text{ is set of all Cover Images}\} \\
&\mathbb{S} = \{S: S \text{ is set of all Stego Images}\} \\
&\mathbb{I} = \{I: I \text{ is set of all Information}\} \\
&\Psi = \{C, S, I, F, F^{-1}\} \text{ and } \Psi \in \Phi \text{ iff } (C, I) \in \mathbb{C} \text{ X } \mathbb{I}
\end{aligned}
\tag{1}
$$

2.2 Security of Stego Algorithm

Susceptibility to steganalysis of any stego algorithm depends upon its Security. As pointed by *Cachin in his Information theoretic model* [2] *and Zollner et.al* in *Modeling the security of steganographic systems* [3] the stego-algorithm {□ , □$^{-1}$} ∈ Φ is said to be ε-secure (ε ≥ 0) if the relative entropy (given by H(Pc||Ps)) between the probability distributions (Probability Mass Function) of cover-image C ∈ ℂ and the stego-image S ∈ 𝕊 given as Pc and Ps respectively is at most ε for every C , S and I in Φ. The security of Stego Algorithm {□ , □$^{-1}$} ∈ Φ is same as security of Universal Stego System Φ and are represented as {□ , □$^{-1}$}(α) or Φ(α) respectively. Therefore {□ , □$^{-1}$}(α) and Φ(α) are one and the same.

$$
\begin{gathered}
\text{If } \{F, F^{-1}\}(\alpha) \text{ or } \Phi(\alpha) - \varepsilon \text{ then} \\
H(Pc||Ps) = \sum Pc \log_2 \frac{Pc}{Ps} \leq \varepsilon \\
(\forall\, C \in \mathbb{C} \textit{ and } \forall\, S \in \mathbb{S} \textit{ where } \mathbb{C} \in \Phi \text{ and } \mathbb{S} \in \Phi\,) \\
(\,0 \log \tfrac{0}{0} = 0,\ p \log \tfrac{p}{0} = \infty \text{ and } p \log \tfrac{0}{p} = -\infty\,)
\end{gathered}
\tag{2}
$$

The security of any Stego-System Ψ = {□ , □$^{-1}$$_{,}$ C, S, I} is given as Ψ(α) and is ε secure (that is Ψ(α) = ε) if H(Pc||Ps) = ε. But this has very narrow connotation as Stego-Algorithm {□ , □$^{-1}$} has to operate not just on C, S and I but on every C ∈ ℂ , every S ∈ 𝕊 and every I ∈ 𝕀. But still the concept of security of any Stego-System Ψ = {□ , □$^{-1}$$_{,}$ C, S, I}forms the basic building block of the concept of security of any Stego-Algorithm { □ , □$^{-1}$} in Universal Stego System Φ = { □ , □$^{-1}$$_{,}$ ℂ , 𝕊, 𝕀 }. This is because any stego algorithm {□ , □$^{-1}$} ∈ Φ is ε secure (ie {□ , □$^{-1}$}(α) or Φ(α) = ε) then maximum value of security of any Stego-System Ψ ∈ Φ (given as Ψ(α)) can be ε for some Ψ ∈ Φ.
Mathematically this can be written as:

$$
\{F, F^{-1}\}(\alpha) \text{ or } \Phi(\alpha) = \text{MAX}\ (\ \Psi_i(\alpha))\quad \forall \Psi_i \in \Phi
\tag{3}
$$

Thus the security of Stego Algorithm {□ , □$^{-1}$} or Universal Stego System Φ is defined in terms of Stego System Ψ_i ∈ Φ. According to *Cachin* a stego-system is perfectly secure if H(Pc||Ps) = 0, which is possible only when Pc = Ps and in such cases receiver is unable to distinguish between C and S as their probability distributions are same and this represents the Shannon's notion of perfect secrecy for cryptosystems[4]. However *Chandramouli et.al* in *Steganography Capacity: A Steganalysis Perspective* [4] have pointed that this definition of Security of stego-system is purely theoretical in nature because it assumes the Cover-object C to be perfectly random. But in reality the Image is not random and in some cases it is possible to steganalyse the image even if the probability distributions of the C and S are same. Hence in addition to parameter ε some more parameters of security of any Universal stego system are devised.

2.2 Preliminaries and Definition

Using Cachin's Information theoretic model[3] and Chandramouli's Mathematical formulation of a Steganalytic Problem[6] and extending both to Image based stego-system a method is devised for representing this system mathematically. Based on this mathematical model a technique is devised for steganlaysis of the stego image.

Before we proceed to mathematical model of Image based stego-system we have to mathematically define the preliminary concepts to be used in this model.

Definition 1 (Image)

Every digital image is collection of discrete picture elements or pixels. Let M be any digital image with N pixels. So any particular pixel of image M is represented as M(z) and z can be any value from 1 to N. This M(z) can be a gray level intensity of the pixel in gray scale image or RGB or YCbCr value of the pixel in a color Image. Thus M(z) can be a set {R(z),G(z),B(z)} or equivalent gray scale representation or (R(z)+G(z)+B(z))/3. But it is always better to consider each R, G and B components individually because the averaging effect cause loss of vital steganographic information. Further < {M},m > is multiset of Image M such that M(z) ∈ {M} for every z = 1 to N and m is a vector corresponding to the occurrence or count of every element M(z) in {M}. Mathematically an image M with N pixels is:

$$\begin{array}{l}
\textit{For any Image}\ \ \mathrm{M}\ \textit{with}\ \mathrm{N\ pixels} \\
\mathrm{M(z)\ \ represents\ its\ pixels}\ \ \forall \mathrm{z} : 1 \leq \mathrm{z} \leq \mathrm{N} \\
\mathrm{M(z)} - \{\mathrm{R(z), G(z), B(z)}\}\ \mathrm{or}\ \ \mathrm{(R(z)+G(z)+B(z))/3} \\
\{\mathrm{M}\} - \{\mathrm{M(z): z -1\ to\ N}\} \\
\mathrm{m} - \textit{occurrence of any particular}\ \ \mathrm{M(z)} \in \{\mathrm{M}\} \\
< \{\mathrm{M}\},\mathrm{m} > \mathrm{is\ multiset\ representing\ image\ M}
\end{array} \qquad (4)$$

Definition 2 (Identical Images)

Two images M and L with N pixels are said to be identical (represented as M ≡ L) if they have pixel to pixel match. This means that two images are identical and absolutely same. Thus their difference image D = M-L will be a pure black image corresponding to zero matrix.

$$\mathrm{M} \equiv \mathrm{L} \Longrightarrow \mathrm{M(z)} = \mathrm{N(z)} \quad \forall \mathrm{z}: 1 \leq \mathrm{z} \leq \mathrm{N} \qquad (5)$$

Definition 3 (Probability distribution of Image)

Probability distribution or Probability Mass Function represented as P(M) for image M = < {M},m > is a multiset <{M}, m' > where m' = $\frac{m}{\mathrm{n}(<\{M\},m>)}$ and n(< {M}, m >) is cardinality (*number of elements*) of multiset of the image M or simply total number of pixels in M. The same is explained mathematically in (6).

$$\begin{array}{l}
\textit{For any Image}\ \ M = <\{M\},m> \\
P(M) = <\{M\},\ m'> \\
m' = \frac{\mathrm{m}}{\mathrm{n}(<\{M\},m>)}
\end{array} \qquad (6)$$

Definition 4 (Macro statistically Same Images)

Two images M and L with N pixels are said to be Macro Statistically Same (represented as M ~ L) if they have equal entropy, energy, contrast ratio, brightness and same histograms. However this does not mean that they are having pixel to pixel match and may not be identical. It simply means that the probability distributions of their pixels are equal. Thus if M ~ L then <{M},m> = <{L},l> or in terms of probability distribution P(M) = P(L). In other words images M and L will have same number of occurrence of any certain pixel intensity but it is not necessary that M(z) = N(z) for any particular z from 1 to N in the image. Thus

$$\begin{array}{l}
\mathrm{M} \sim \mathrm{L} \Longrightarrow < \{\mathrm{M}\},\mathrm{m} > = < \{\mathrm{L}\},\mathrm{l} >\ \ \mathrm{or}\ \mathrm{P(M)} = \mathrm{P(L)}. \\
\mathrm{Also}\ \mathrm{M} \sim \mathrm{L} \nRightarrow \mathrm{M} \equiv \mathrm{L}.
\end{array} \qquad (7)$$

Definition 5 (Neighborhood or Locality of Pixel)

If ℓ(M(z)) is said to be set of neighboring pixels of any pixel M(z) in image M. Then any n_i ∈ ℓ(M(z)) will be such that $d(n_i, \mathrm{M(z)}) \leq \lambda$ where *d* is a function which calculates distance (can be Euclidean, City-Block, Chess Board or any other type depending upon the steganographic algorithm) between its inputs (ie n_i and M(z)) and λ is measurement of degree of neighbourhood and should be minimum (Generally equal to 1 pixel) but also depends upon the steganographic algorithm used by stegosystem Ψ. Mathematically this can be represented as:

$$\ell(M(z)) = \{M(x) : M(x) \in M \text{ and } d(M(x), M(z)) \leq \lambda\} \qquad \textbf{(8)}$$

In Fig 1 an arbitrary pixel Y is shown with its neighbors P, Q, R, S, T, U, V and W. We represent this pixel Y as Ẏ in mathematical notation. Thus ℓ(Ẏ) = {P, Q, R, S, T, U, V ,W} is set of neighboring pixels of pixel Y. Here λ = 1 and distance function *d* calculates Chess Board Distance.

P	**Q**	**R**
S	**Y**	**T**
U	**V**	**W**

Fig 1 Pixel Y

Definition 6 (Adjacent Neighbors of Pixel)

Set of Adjacent Neighbors of a pixel M(z) is given as $\mathcal{A}$ (M(z)). Thus $\mathcal{A}$ (M(z)) is a collection of set {M(x), M(y)} such that M(x) ∈ ℓ(M(z)) and M(y) ∈ ℓ(M(z)) and they are adjacent i.e *d* (M(x) , M(y)) = 1 where *d* is a function which calculates distance. Mathematically:

$$\mathcal{A}(M(z)) = \{\{M(x),M(y)\} : M(x) \in \ell(M(z)) \text{ and } M(y) \in \ell(M(z)) \text{ and } d(M(x), M(y)) = 1\} \qquad \textbf{(9)}$$

In Fig 1 for an arbitrary pixel Y with ℓ(Ẏ) = {P, Q, R, S, T, U, V ,W} the $\mathcal{A}$(Ẏ) = {{P,Q}, {Q,R)}, {R,T}, {T,W}, {W,V},{V,U},{U,S},{S,P}}.

Definition 7 (Pixel Aberration)

Pixel Aberration of any Pixel M(z) from its neighborhood ℓ(M(z)) in terms of Standard Deviation of ℓ(M(z)) is given as δ (M(z) , ℓ(M(z))). It is a quantifier which gives the idea of the amount of deviation of the pixel from its neighborhood. In any natural image a pixel M(z) is expected to be as much different from its neighborhood as the adjacent pixels in ℓ(M(z)) themselves are.

For any pixel M(z) the mean of its absolute difference from its neighborhood ℓ(M(z)) is given as $\overline{(M(z), \ell(M(z)))}$. And the set representing the absolute differences of the adjacent neighbors of M(z) among themselves is given as $\mathcal{D}(\mathcal{A}$ (M(z))). The mean of the values of $\mathcal{D}(\mathcal{A}$ (M(z))) is given as $\overline{D(A\ (M(z)))}$ and Standard Deviation of the values of $\mathcal{D}(\mathcal{A}$ (M(z))) is given as $\sigma(\mathcal{D}(\mathcal{A}$ (M(z)))) . Since M(z) is also a immediate neighbor of ℓ(M(z)) so $\overline{(M(z), l(M(z)\ ))}$ must be within the limits of standard deviation of $\mathcal{D}(\mathcal{A}$ (M(z))) and mean of $\mathcal{D}(\mathcal{A}$ (M(z))). This degree of deviation of M(z) from its neighbors ℓ(M(z)) in terms of $\sigma(\mathcal{D}(\mathcal{A}$ (M(z)))) and $\overline{D(A\ (M(z)))}$ is quantified as δ (M(z) , ℓ(M(z))) and hence it represents the aberration in the pixel M(z).

In terms of Fig 1 the mean of the differences of pixel Y with its neighbors i.e. elements of ℓ(Y) is given as Y-P,Y-Q, Y-R, Y-S, Y-T, Y-U, Y-V and Y-W and should be close to the differences of the adjacent pixels in ℓ(Ẏ) i.e. difference of the elements of {P,Q},{Q,R)},{R,T},{T,W}{W,V},{V,U},{U,S} and {S,P} or simply P-Q, Q-R, R-T, T-W, W-V, V-U, U-S and S-P. Thus $\overline{(M(\dot{Y}), \ell\left(M(\dot{Y})\right))}$ is mean of modulus of Y-P, Y-Q, Y-R, Y-S, Y-T, Y-U, Y-V and Y-W and $\mathcal{D}(\mathcal{A}$ (Ẏ)) = {modulus of P-Q, Q-R, R-T, T-W, W-V, V-U, U-S and S-P}. So aberration in pixel Y with respect to its neighborhood ℓ(Ẏ) given as δ (Ẏ , ℓ(Ẏ)) should be within the limits of standard deviation of $\mathcal{D}(\mathcal{A}$(Ẏ)) and $\overline{D(A(\dot{Y}\ ))}$.

Mathematically:

$$\overline{(M(z), \ell(M(z)))} = \frac{1}{n(\ell(M(z)))} \sum_{p \in \ell(M(z))} |p - M(z)|$$

$$\mathcal{D}(\mathcal{A}(M(z))) = \{|x - y| : (x,y) \in \mathcal{A}(M(z))\}$$

$$\delta\left(M(z), \ell(M(z))\right) = \frac{\overline{(M(z), \ell(M(z)))} - \overline{D(\mathcal{A}(M(z)))}}{\sigma(\mathcal{D}(\mathcal{A}(M(z))))} \qquad \textbf{(10)}$$

Definition 8 (Pixel Aberration of Image)

In any image M with N pixels the Pixel aberration of image M is given as $\delta(M)$. It is the weighted mean of the modulus of the pixel aberrations of the pixels of the entire image M. Since for any image M the $\delta\left(\text{M(z)}, \ell(\text{M(z)})\right)$ is the measure of deviation of M(z) from its neighborhood $\ell\left(\text{M(z)}\right)$ in terms of standard deviation so majority of pixels have this values located close to zero and approximately more than 68% of the pixels have pixel aberration within $\pm$ 1 *(as per 3 Sigma or 68-95-99.7 rule of Statistics)*. Hence the simple mean of $\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right)$ is very close to zero and is insignificantly small for all images. Since by pixel aberration analysis we have to identify those images which have larger pixel aberrations so as a remedy very small weights are assigned to less deviated values (majority of pixels which have low pixel aberration values) and larger weights are assigned to more deviated values (few counted pixels have large pixel aberrations). Thus value of $\delta(M)$ for the

Image M with N pixels is given as:

$$\delta(M) = \frac{\sum_{\substack{z=1 \\ M(z)\in M}}^{N} \left|\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right| \times W(z)}{\sum_{\substack{z=1 \\ M(z)\in M}}^{N} W(z)}$$

(11)

The weight W(z) for the pixel M(z) is much smaller for small values of $\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right)$ and quite large for big values of $\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right)$. Thus W(z) is large for pixel having greater pixel aberration and very small for pixels having lesser pixel aberration. Such weights can be computed by taking cube of the value of pixel aberration in terms of the standard deviation. In other words the weight W(z) for any Pixel M(z) in image M is given as

$$\mathrm{W(z)} = \left|\frac{\delta\left(\mathrm{M(z)},\ell\left(\mathrm{M(z)}\right)\right) - \mathrm{MEAN}\ {}_{\mathrm{Z=1}}^{\mathrm{Z=N}}\left(\delta\left(\mathrm{M(z)},\ell\left(\mathrm{M(z)}\right)\right)\right)}{\mathrm{STD}\ {}_{\mathrm{Z=1}}^{\mathrm{Z=N}}\left(\delta\left(\mathrm{M(z)},\ell\left(\mathrm{M(z)}\right)\right)\right)}\right|^{3}$$

$$\mathrm{W(z)} = \left|\frac{\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right) - \frac{1}{\mathrm{n(M)}}\sum_{z=1}^{z=\mathrm{n(M)}} \delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right)}{\sqrt[2]{\left(\frac{1}{\mathrm{n(M)}}\sum_{z=1}^{z=\mathrm{n(M)}} \delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right)^{2}\right) - \left(\frac{1}{\mathrm{n(M)}}\sum_{z=1}^{z=\mathrm{n(M)}} \delta\left(\mathrm{M(z)}, \ell\left(\mathrm{m(z)}\right)\right)\right)^{2}}}\right|^{3}$$

(12)

Although we may avoid taking weighted mean and we can use simple mean but for that we have to consider only those values of $\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)$ for determining mean which are above or below certain threshold $\pm\, \check{\tau}$ and rest of the values can be filtered. This value of $\check{\tau}$ is generally given in terms of standard deviation of $\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)$ from z = 1 to N and in represented as τ. Thus Mean Pixel Aberration of Image M at threshold **τ** is represented as $\boldsymbol{\delta}(\boldsymbol{M},\ \boldsymbol{\tau})$ and mathematically defined as:

$$\check{\tau} = MEAN\,{}_{Z=1}^{Z=N}\left(\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right) \pm \tau \times STD_{Z=1}^{Z=N}\left(\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right)$$

$$\tau = \frac{\check{\tau} - MEAN\,{}_{Z=1}^{Z=N}\left(\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right)}{STD_{Z=1}^{Z=N}\left(\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right)}$$

$$\delta(M,\tau) = \frac{1}{N}\sum_{\substack{\left|\delta\left(M(z),\ell\left(M(z)\right)\right)\right| \geq \check{\tau} \\ M(z)\in S \quad \forall z:\ 1\leq z\leq N}} \left|\ \delta\left(M(z), \ell\left(M(z)\right)\right)\ \right|$$

(13)

Thus this value of τ depends on smoothness of the cover image and the type of aberration we are interested in. In unsmooth cover images the differences of the pixels with their neighbors is quite large (for example an image of a Forest or Valley) and hence the value of $\delta(M,\tau)$ at larger τ represents the mean of only those deviations which are larger than τ. Whereas for smooth cover images like clear blue sky the aberration is already very low and hence smaller value of τ produces good result.

Definition 9 (Range of Pixel Aberration in the Image)

In any image M with N pixels the Range of Pixel aberration of image M is given as $\mathcal{R}(M)$. It is the difference of the Maximum Pixel Aberration ($\mathcal{R}(M)^{\uparrow}$ in the image M and Minimum Pixel Aberration ($\mathcal{R}(M)_{\downarrow}$ in the Image M.

Thus Mathematically the same can be expressed as:

$$(\mathcal{R}(M))^{\uparrow} = \max_{1\leq z\leq N}\ \left(\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right)$$
$$(\mathcal{R}(M))_{\downarrow} = \min_{1\leq z\leq N}\ \left(\delta\left(\mathrm{M(z)}, \ell\left(\mathrm{M(z)}\right)\right)\right)$$
$$\mathcal{R}(M) = (\mathcal{R}(M))^{\uparrow} - (\mathcal{R}(M))_{\downarrow}$$

(14)

Definition 10 (Maximum Deviation in the Pixel Aberration of the Image)

In any image M with N pixels the Maximum Pixel Aberration in M given as Δ(M) is the maximum pixel aberration in absolute terms in the image M. τ corresponding to Δ(M) is represented as $\mathcal{T}$. Thus

$$\Delta(M) = \text{MAX}\left(\left|\ (\mathcal{R}(M))^{\uparrow}\right|, \left|(\mathcal{R}(M))_{\downarrow}\right|\right) \quad \textbf{(15)}$$

$$\mathcal{T} = :\ \tau = \Delta(M)$$

$$\mathcal{T} = \frac{\Delta(M) - MEAN_{z=1}^{z=N}\left(\delta\left(M(z), \ell(M(z))\right)\right)}{STD_{z=1}^{z=N}\left(\delta\left(M(z), \ell(M(z))\right)\right)} \quad \textbf{(16)}$$

2.3 Detailed Mathematical Model of any Image based Stego Algorithm

In Equation 2 it has been very clearly shown that security of any stego system Ψ = {□ , □$^{-1}$, C, S, I} is the basic building block of security of the stego-algorithm {□ , □$^{-1}$}. So for the sake of simplicity it is better to operate on stego-system only. Let Ψ = {□ , □$^{-1}$, C, S, I} be any Image Steganographic System with □ , □$^{-1}$, C, S and I having the same meaning as mentioned in previous section. Thus S = □ (C, I) and I = □ $^{-1}$(S) also holds well. Now let us assume that Cover Image C consists of N discrete pixels represented by C(1), C(2), … C(N). Although cover image C is meant for storing Information I. But any arbitrary pixel C(z) of C can at max store only a limited part of Information I. Let this small part of I stored in C(z) be represented as I(z). Thus our Information I can be broken to K parts represented by I(1), I(2) …I(K), K ≤ N such that any I(z) is the information stored in any particular pixel C(z) for any z ≤ N. If information I is smaller than the cover-image C ie if K < N then the remaining I(z) from z = K+1 to N can be thought to be empty or Null set and given as I(z) = { } for z = K+1 to N. Thus the cardinality of both I and C (given as n(I) and n(C) respectively) is made equal i.e. N. Since S = □ (C, I) so corresponding toevery C(z) in C we have a unique S(z) in S. Using the notations of Set Theory the same is mathematically written in (17).

$$\begin{array}{l}
\Psi = \{C, S, I, F, F^{-1}\} \\
n((\{C\}, c)) = N \textit{ and any pixel of } C \text{ is } C(z)\ \forall z: 1 \le z \le N \\
S = F(C, I) \\
I = F^{-1}(S) \\
I(z) \textit{ is Information stored in any particular Pixel } C(z) \\
(\{C\}, c) = \cup_{z=1}^{N} C(z) \text{ and } I = \cup_{z=1}^{K} I(z) \text{ where } K \le N \\
\textit{In order to have } n(<\{C\}, c>) = n(I) = N \textit{ even if } K < N \\
\textit{we have to assume } I(z) = \{\ \}\ \forall z: K+1 \le z \le N \\
\textit{Thus after having cardinality of } C \textit{ and } I \textit{ equal we can say} \\
\qquad \forall C(z) \in C\ \exists \text{ unique } I(z) \in I. \\
\textit{Also since } S = F(C, I) \text{ so } \forall\ C(z) \in C\ \exists \textit{ unique } S(z) \in S. \\
\textit{Thus } <\{S\}, s> = \cup_{z=1}^{N} S(z)
\end{array} \quad \textbf{(17)}$$

The stego-function □ :(C, I) → S can be redefined at pixel level as S(z) = α(z) [C(z) ● I(z)] where ● is any operator used by stego-funtion □ acting over C and I to produce S and α(z) ≥ 0 is factor which strengthens Ψ for z = 1 to N. Thus α(z) ∀z: 1≤ z ≤ N is strengthening factor of stego system Ψ and helps it in achieving secure Ψ (ie α(z) for z = 1 to N is the factor which helps in achieving Ψ(α)).

The inverse stego function □$^{-1}$:(S) → I can be redefined at pixel level as I(z) = Θ (S(z)) where Θ is a unary operator used by □$^{-1}$ acting on S to produce I and hence indirectly C also. Thus algorithmically unary operator Θ is inverse of the operator ●.

2.3.1 Parameters for Measuring Strength of Stego Algorithm

Strengthening Factor α(z) ∀z: 1≤ z ≤ N, keeps S(z) such that it is least susceptible to any steganalysis attacks by making S perfectly resemble an Innocent Image i.e. without any distortions. Therefore this α(z) has to meet four main requirements which are explained next.

Requirement 1

Using operator ● the α(z) should map C(z) and I(z) to S(z) in such a way that relative entropy of cover and stego image given as H(P(C) || P(S)) should be minimum possible. Here P(C) is probability distribution of C and P(S) is probability distribution (Probability Mass Function) of S and H(P(C) || P(S)) is relative entropy of P(C) with P(S). This requirement is derived from equation 1 mentioned in section 2.2. This simply means that macro statistical parameters of the Cover-Image C and Stego-Image S should be almost same or in terms of relative entropy should be minimum possible. This requirement is extension of Cachin's Information theoretic model in terms of α. Mathematically this can be expressed as

□(z) should be such that:

$$H(P(C) \| P(S)) = \sum P(C) \log_2 \frac{P(C)}{P(S)} = \varepsilon \quad \textbf{(18)}$$

Where P(C) and P(S) are probability distribution of C(z) and S(z) ∀z: 1≤ z ≤ N and such a stego-system is said to be ε Secure.

In order to achieve this requirement the stego function □ :(C, I) → S willmacro-statistically redistribute the pixels of C in such a way that even though corresponding pixels C(z) and S(z) may not be same but still probability distribution of pixels C(z) in C and S(z) in S for z = 1 to N will remain same that is C ~ S will be achieved. Thus by fulfilling this requirement (assuming ε = 0) the Cover Image and the Stego Image will have same Histogram, Brightness, entropy, energy, contrast ratio and all other macro statistical parameters even if C ∓ S that is C(z) ≠ S(z) ∀z:1≤ z ≤ N.

Requirement 2

If only Requirement 1 is met we may have a situation where even though the cover-image may look macro-statistically same (in terms of Histogram, Brightness, entropy, energy, contrast ratio etc) as stego-image but still they may have significantly different pixel to pixel correspondence between C and S. I.e. any particular pixel S(z) of S may be considerably different from C(z) of C thus revealing the distortions in S(z) and hence making S susceptible to Steganalysis. Thus in addition to macro-statistical redistribution of the pixels of cover image (as mentioned in Requirement 1) the stego-algorithm must redistribute the pixels of the neighborhood of every pixel C(z) in C (i.e. ∀z: 1≤ z ≤ N) is such way that two corresponding pixels C(z) and S(z) should have same probability distribution of their neighborhood. Thus α(z) should meet another requirement:

Using operator ● the α(z) should map C(z) and I(z) to S(z) in such a way that the relative entropy between the Neighborhood of C(z) and S(z) (or Local Relative Entropy) should be least possible ∀z: 1≤ z ≤ N. Thus any Image based Stego-System Ψ is said to be ξ Secure if the mean of the relative entropies of the neighborhood of C(z) and S(z) for all C(z) in C and S(z) in S (that is ∀z: 1≤ z ≤ N) is ξ. Thus α(z) should be such that ξ is minimum where ξ is given as

$$\frac{1}{N}\sum_{z=1}^{z=N} \mathbf{H}\big(\mathbf{P}(\ell(\mathbf{C}(\mathbf{z})))\,||\,\mathbf{P}(\ell(\mathbf{S}(\mathbf{z})))\big)$$

$$=\frac{1}{\mathbf{N}}\sum_{z=1}^{z=N} \mathbf{P}(\ell(\mathbf{C}(\mathbf{z})))\log_2\frac{\mathbf{P}(\ell(\mathbf{C}(\mathbf{z})))}{\mathbf{P}(\ell(\mathbf{S}(\mathbf{z})))} = \xi \qquad \textbf{(19)}$$

Here $P(\ell(C(z)))$ is probability distribution of the pixels in the neighbourhood of pixel C(z) and $P(\ell(S(z)))$ is probability distribution of the pixels in the neighbourhood of pixel S(z).

Requirement 3

Most spatial domain Stego Algorithms distribute the entire information in large number of pixels and as a result the changes in the pixel values are very small and unnoticeable but in this process large number of the pixels in the image change and hence the relative entropy of the stego-image and cover-image increases due to considerable change in probability distribution of pixels in the image. Security of such algorithms can be defined by Requirement 1 and Requirement 2 that is ε and ξ.

But there are certain Image Stego Algorithms which concentrate the information in very few pixels. As a result the change in pixels values of these few pixels is very large and hence quiet perceptible even though the probability distribution of pixels is not much disturbed. In case of such algorithms even if ε and ξ are very small the stego-image may have few grains in last few rows (grains are due to large and perceptible changes in those few pixels and changes in the bottom most pixel usually goes unnoticed due to psycho-visual weaknesses of human eye) and are susceptible to steganalysis. In any natural Image a pixel P is almost same as its neighbors. Therefore on an average C(z) will not be very different from ℓ(C(z)) for most values in z = 1 to N. Thus α(z) should meet another requirement:

Using operator ● the α(z) should map C(z) and I(z) to S(z) in such a way that any particular pixel should not change much. Thus the difference between Weighted Mean of the Pixel Aberration of Stego-Image S from Cover-Image C (Definition 8) should be minimum possible. The weighted mean pixel aberration δ can be calculated by either obtaining the Maximum of the red , green and blue values or by taking the average of red, green and blue values. Hence mathematically the difference between Weighted Mean of the Pixel Aberration of Stego-Image S from Cover-Image C is represented as $\grave{e}_{\mathrm{MAX}}$ and $\grave{e}_{\mathrm{MEAN}}$ and given as

$$\grave{\boldsymbol{e}}_{\mathbf{MAX}} = \boldsymbol{MAX}_{\mathbf{RGB}}(\,\boldsymbol{\delta}(\boldsymbol{S})) - \boldsymbol{MAX}_{\mathbf{RGB}}\,(\,\boldsymbol{\delta}(\boldsymbol{C}))$$

or

$$\grave{\boldsymbol{e}}_{\mathbf{MEAN}} = \boldsymbol{MEAN}_{\mathbf{RGB}}(\,\boldsymbol{\delta}(\boldsymbol{S})) - \boldsymbol{MEAN}_{\mathbf{RGB}}\,(\,\boldsymbol{\delta}(\boldsymbol{C})) \qquad \mathbf{20}$$

The same can be alternatively represented by finding the difference between the mean pixel aberration of Cover Image C and Stego-Image S considering only those values of pixel aberrations (of $\delta\big(\,C(z), \ell(C(z))\big)$ and $\delta\big(\,S(z), \ell(S(z))\big)$ for z = 1 to N) in entire image which are above a certain threshold $\pm\,\check{\boldsymbol{\tau}}$ **and given**

as $\delta(C,\tau)$ and $\delta(S,\tau)$ Thus α(z) should be such that the difference between the pixel aberrations of Stego-Image and Cover-Image at threshold τ (in terms of standard deviation it corresponds to pixel aberration value of $\pm\check{\boldsymbol{\tau}}$) should be minimum possible and given as $e(\tau)$.

In unsmooth cover images the aberration is already very high and addition of information brings further more aberrations (in some efficient stego-algorithms it may reduce the aberrations too) so if the value of τ is kept large then $e(\tau)$ will be measure of differences in only those large aberrations. Whereas in smooth cover images the aberration is quite low and hence lower value of τ is advisable. In some cases we may get a value of $e(\tau)$ as negative which indicates that at threshold τ the Stego Image has lesser aberration then the cover image.

Certain steganographic algorithms hide the data very efficiently and as a result only few counted pixels have aberration beyond the prescribed limit. In such cases determination of weaknesses in these algorithms using only fixed value $e(\tau)$ goes unnoticed due to averaging effect of large number of pixels having much lower pixel aberration. Moreover $e(\tau)$ has different value at every τ. Thus a better estimate of $e(\tau)$ can be $\check{e}$ which is the mean of $e(\tau)$ for continuously increasing value of τ from 0 to that value of τ which corresponds to modulus of Maximum Pixel Aberration (Definition 10) in the stego image that is for $\tau = 0$ to $\mathcal{T}$.

$$\boldsymbol{e(\tau) = \delta(S,\tau) - \delta(C,\tau)}$$

$$\mathcal{T} = \tau : \check{\tau} = \Delta(\mathrm{M})$$

$$\check{e} = \frac{1}{\mathcal{T}}\int_0^{\mathcal{T}} e(\tau)\,d\tau$$

(21)

Since calculating the value of $\check{e} = \frac{1}{\mathcal{T}}\int_0^{\mathcal{T} = \tau : \check{\tau} = \Delta(\mathrm{M})} e(\tau)\,d\tau$ is practically very expensive in various accords of time and computation power. So more practical way to estimate of $\bar{e}$ can be based on taking means of $e(\tau)$ at any chosen discrete values of τ for example like τ = 0, 1/8 $\mathcal{T}$, 2/8 $\mathcal{T}$, 3/8 $\mathcal{T}$ ... $\mathcal{T}$.

Thus as an indicator of requirement 3 either $\grave{e} = \delta(S) - \delta(C)$ or $\check{e} = \frac{1}{\mathcal{T}}\int_0^{\mathcal{T} = \tau : \check{\tau} = \Delta(\mathrm{M})} e(\tau)\,d\tau$ can be considered. But generally the difference of the weighted means of the pixel aberration of cover image and stego image as given as $\grave{e}$ in (20) will be preferable although this may vary from algorithm to algorithm and situation to situation. Whatever the value we consider for obtaining this difference i.e. either $\grave{e}$ or $\check{e}$ has to be represented by $\bar{e}$ in the holistic representation of the requirement 4 in the steganographic system. Thus $\bar{e}$ is either $\grave{e}$ or $\check{e}$.

Requirement 4

Another very good indicator of presence of anomaly in the pixels of the image is Range of Pixel Aberration $\mathcal{R}(M)$ in the Image (Definition 9). Bigger value of $\mathcal{R}(M)$ in spite of lower values of $e(\tau)$ indicates that only very few counted pixels have aberration much beyond the prescribed limit and hence the given image could be a potential stego-image. Thus using operator ● the α(z) should map C(z) and I(z) to S(z) in such a way that Range of Pixel Aberration in Cover Image must not be very different from the Range of Pixel Aberration in the Stego image. Thus the difference of Range of Pixel Aberration of Cover and Stego Image should be minimum possible and given as €.

$$\text{€} = \frac{\mathcal{R}(S) - \mathcal{R}(C)}{\mathcal{R}(C)} \qquad \textbf{(22)}$$

Thus € is the indicator of percentage change in the Range of Pixel Aberration in Cover Image after embedding the data in it.

In colored Image the € value is different for Red, Green and Blue components of the Image. But we can't take average of the three as € value represents the Range of Pixel Aberration and hence for RGB image, this € is given as

$$\text{€} = \mathrm{MAX}\,(\text{€}_{\mathrm{RED}}, \text{€}_{\mathrm{GREEN}}, \text{€}_{\mathrm{BLUE}})$$

(23)

Also it is better if we mention the color component which has maximum € in RGB Image.

2.4 Holistic Representation of Stego System and Universal Stego System Mathematically

Based on these four requirements of α with regards to the Strength of any Steganographic System Ψ we may define security of Ψ by four tuple < ε, ξ, $\bar{e}$,€ > and say Ψ(α) = < ε, ξ, $\bar{e}$,€ > secure.
Thus Image based Universal stego system Φ = { □ , □$^{-1}$, ℂ , 𝕊, 𝕀 } with any Stego System Ψ = {C, S, I, □ , □$^{-1}$} such that Ψ ∈ Φ can be more elaborately defined at pixel level as

$$\begin{aligned}&\Phi = \{\, \mathbb{C}, \mathbb{S}, \mathbb{I}, \Phi(\text{Algorithm}), \Phi(\alpha)\} \text{ and}\\ &\Psi = \{C, S, I, \Psi(\text{Algorithm}), \Psi(\alpha)\}\\ &\textit{In other words}\\ &\Phi = \{\, \mathbb{C}, \mathbb{S}, \mathbb{I}, < \bullet, \Theta >, < \varepsilon, \xi, \bar{e}, € >\} \text{ and}\\ &\Psi = \{C, S, I, < \bullet, \Theta >, < \varepsilon, \xi, \bar{e}, € >\}\end{aligned} \quad \textbf{(24)}$$

Here Stego-Algorithm of Φ or Φ (Algorithm) = $< \bullet, \Theta >$ where Φ (□) = ● and Φ ($□^{-1}$) = Θ and Strength of Φ given as Φ (α) = $< \varepsilon, \xi, \bar{e}, € >$.

Since handling of four different values of Φ(α) is quite difficult so four values of Φ (α) = $< \varepsilon, \xi, \bar{e}, € >$ can be reduced in to one value represented as $< \Phi(\alpha) >$ by taking weighted means of their modulus.

$$< \Phi(\alpha) > = \frac{w_1\,|\varepsilon| + w_2\,|\xi| + w_3\,|\bar{e}| + w_4\,|€|}{w_1 + w_2 + w_3 + w_4} \quad \textbf{(25)}$$

The values of these four weights w_1, w_2, w_3, w_4 depends upon the alertness and sensitivity of steganalysis algorithm with respect to the four strength parameters ε, ξ, $\bar{e}$,€ of any steganographic algorithm. In most general cases we assume that the steganalyst is capable of exploiting any of these 4 vulnerabilities and therefore the four conditions have equal importance and hence $w_1 = w_2 = w_3 = w_4$ and therefore the value of $< \Phi(\alpha) >$ becomes simple mean of $< \varepsilon, \xi, \bar{e}, € >$ and given as $< \Phi(\alpha) > = (\varepsilon + \xi + \bar{e} + €)/4$.

The smaller value of $< \Phi(\alpha) >$ indicates that the algorithm Φ is stronger. Thus Image based Universal stego system Φ = { □ , $□^{-1}$, ℂ , 𝕊, 𝕀 } with any Stego System Ψ = {C, S, I, □ , $□^{-1}$} such that Ψ ∈ Φ can also be defined as

$$\begin{aligned}&\Phi = \{\, \mathbb{C}, \mathbb{S}, \mathbb{I}, \Phi(\text{Algorithm}), < \Phi(\alpha) > \}\\ &\textit{and } \Psi = \{C, S, I, \Psi(\text{Algorithm}), < \Psi(\alpha) > \}\end{aligned} \quad \textbf{(26)}$$

2.5 Steganalysis is Always Possible

In this section a theorem is given which proves that every stego system is susceptible to steganalysis.

Theorem: No Image based Stego Algorithm (Universal Stego System) is fool proof.

Assumption

Let there be any fool proof Universal stego system Φ = { ℂ , 𝕊, 𝕀 , Φ(Algorithm) , Φ(α)} such that Φ(α) = $< \varepsilon, \xi, \bar{e}, € > = < 0, 0, 0, 0 >$ and Φ(Algorithm) = { □ , $□^{-1}$} capable of exchanging Y distinct and authentic Information $I_1, I_2\, I_3 \ldots I_Y$.

Thus mathematically this assumption can be written as:

$$\begin{aligned}&\Phi = \{\, \mathbb{C}, \mathbb{S}, \mathbb{I}, \Phi(\text{Algorithm}), \Phi(\alpha)\}\\ &\Phi(\alpha) = < \varepsilon, \xi, \bar{e}, € > = < 0, 0, 0, 0 >\\ &\Phi\,(\text{Algorithm}) = < \bullet, \Theta >\\ &\textit{Where } \Phi\,(F) = \bullet \textit{ and } \Phi\,(F^{-1}) = \Theta\\ &\{ I_1, I_2\, I_3 \ldots I_Y \} \in \mathbb{I} \text{ and } I_1 \neq I_2 \neq I_3 \neq \ldots \neq I_Y \textit{ and}\\ &\textit{any } I_X \in \mathbb{I} \text{ is not empty } \forall x:\ 1 \leq x \leq Y\end{aligned} \quad \textbf{(27)}$$

Proof:

Some information $I_k \in \mathbb{I}$ is being exchanged through above assumed Universal stego-system Φ using cover-image C ∈ ℂ of size N. As any $I_X \in \mathbb{I}$ is not empty ∀x: 1≤ x ≤ Y so $I_k(z) \neq \{\ \}$ for at least one z from 1 to N.

As S(z) = α(z) [C(z) ● I_k(z)] and Φ(α) = $< \varepsilon, \xi, \bar{e}, € > = < 0, 0, 0, 0 >$ so S(z) will be such that S(z) = C(z) and hence Stego Image S and Cover Image C are identical or S ≡ C.

Now a different Information $I_m \in \mathbb{I}$ is exchanged through same Universal Stego system Φ with same cover Image C. Again since S(z) = α(z) [C(z) ● I_m (z)] and Φ(α) = $< \varepsilon, \xi, \bar{e}, € > = < 0, 0, 0, 0 >$ so S(z) = C(z). Therefore again S and C are identical or S ≡ C.

Thus for any information $I_x \in \mathbb{I}$ the Universal stego-system Φ is such that S and C are identical and same. But as we know that S = □ (C, I) and I = $□^{-1}$(S) so for every stego-image S there exists a unique Information I.

But in the given case the same stego-image S corresponds to different distinct information $I_1, I_2\, I_3 \ldots I_Y$. Hence we conclude that all information are same i.e. $I_1 = I_2 = I_3 = \ldots = I_x = \ldots = I_{Y-1} = I_Y$.

But this is in contradiction with our assumption that $\{I_1, I_2\, I_3 \ldots I_Y\} \in \mathbb{I}$ and $I_1 \neq I_2 \neq I_3 \neq \ldots \neq I_Y$.

Thus our assumption is wrong and hence Φ(α) = $< \varepsilon, \xi, \bar{e}, € > \neq < 0, 0, 0, 0 >$ and hence $< \Phi(\alpha) >$ is more then 0.

III. Application of the Mathematical Model in Real Scenario for evaluation of Stego Algorithms

Based on the mathematical model developed in Section 2 three different spatial domain steganographic algorithms are evaluated for susceptibility to steganalysis. These three Algorithms are named as Algorithm I, Algorithm II and Algorithm III and represented mathematically as Universal Stego Systems Φ_1, Φ_2 and Φ_3 respectively. These three steganographic algorithms were also used in [1] and are referred in Section 5 of [1] as *Algorithm designed in section 4*, *QuickStego Software* and *Eureka Steganographer* respectively**.** Thus Φ_1(Algorithm) is Algorithm I, Φ_2(Algorithm) is Algorithm II and Φ_3(Algorithm) is Algorithm III. The features of these three algorithms are summarized in Table 1.

For the sake of uniformity (which is required for Evaluation) we use same set of two different cover images for evaluation of Φ_1, Φ_2 and $\Phi_{3.}$ One of them is smooth (has low Pixel Aberration) and other is relatively unsmooth and has high Pixel Aberration and hence named as Smooth and Unsmooth and mathematically represented as **smooth** and **unsmooth** respectively.. Thus set of Cover Images $\mathbb{C}$ = {**smooth**, **unsmooth**} and $\mathbb{C} \in \Phi_1$, $\mathbb{C} \in \Phi_2$ and $\mathbb{C} \in \Phi_3$ and δ(**smooth**) < δ(**unsmooth**). The two cover images smooth and unsmooth are shown in Figure 1. Based on various parameters of Image mentioned in Section 2.2 these two images are summarized in Table 2. These parameters are calculated using MATLAB© Image Processing Tool Box.

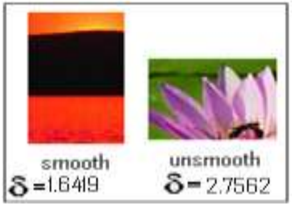

Fig 1 Cover Images $\mathbb{C}$ = {smooth, unsmooth}

In order to maintain uniformity in evaluation of Φ_1, Φ_2 and Φ_3 we embed same Information I using all the three algorithms. This information I is 900 character string of abcdef….z1234 repeated 30 times. Thus I = abcdef….z1234 (30 times) and {I} = $\mathbb{I}$.

Thus mathematically the three Universal Stego Systems are summarized as:

$$\begin{aligned}
&\Phi_1 = \{\ \mathbb{C}\ ,\ \mathbb{S},\ \mathbb{I}\ ,\ \Phi_1(\textbf{Algorithm})\ ,\ \Phi_1(\alpha)\}\\
&\Phi_2 = \{\ \mathbb{C}\ ,\ \mathbb{S},\ \mathbb{I}\ ,\ \Phi_2(\textbf{Algorithm})\ ,\ \Phi_2(\alpha)\}\\
&\Phi_3 = \{\ \mathbb{C}\ ,\ \mathbb{S},\ \mathbb{I}\ ,\ \Phi_3(\textbf{Algorithm})\ ,\ \Phi_3(\alpha)\}\\
&\mathbb{C} = \{\textit{smooth},\ \textit{unsmooth}\}\\
&\mathbb{C} \in \Phi_1\ ,\ \mathbb{C} \in \Phi_2\ \textbf{and}\ \mathbb{C} \in \Phi_3\ .\\
&\{\mathbf{I}\} = \mathbb{I}\\
&\mathbf{I} = \textbf{abcdef....z1234 (30 times)}\\
&\mathbb{I} \in \Phi_1,\ \mathbb{I} \in \Phi_2\ \textbf{and}\ \mathbb{I} \in \Phi_3
\end{aligned} \qquad \textbf{(28)}$$

Using two cover Images $\mathbb{C}$ = {**smooth**, **unsmooth**} and three Universal Stego Systems Φ_1, Φ_2 and Φ_3 we obtain Six Stego-Systems given as Ψ_{1S}, Ψ_{1U}, Ψ_{2S}, Ψ_{2U}, Ψ_{3S} and Ψ_{3U} . These six stego systems are mathematically given as:

$$\begin{aligned}
&\textbf{Stego-System}\ \Psi_{1S}\text{: } \Psi_{1S} \in \Phi_1\ \textbf{and}\\
&\Psi_{1S} = \{\ \textit{smooth}\ ,\ S_1^{\ S}\ ,\ \mathbf{I},\ \Psi_{1S}\ (\textbf{Algorithm})\ ,\ \Psi_{1S}(\alpha)\}\}\\
&\textbf{Stego-System}\ \Psi_{1U}\text{: } \Psi_{1U} \in \Phi_1\ \textbf{and}\\
&\Psi_{1U} = \{\ \textit{unsmooth}\ ,\ S_1^{\ U}\ ,\ \mathbf{I},\ \Psi_{1U}\ (\textbf{Algorithm})\ ,\ \Psi_{1U}(\alpha)\}\}
\end{aligned} \qquad \textbf{(29-A)}$$

$$\begin{aligned}
&\textbf{Stego-System}\ \Psi_{2S}\text{: } \Psi_{2S} \in \Phi_2\ \textbf{and}\\
&\Psi_{2S} = \{\ \textit{smooth}\ ,\ S_2^{\ S}\ ,\ \mathbf{I},\ \Psi_{2S}\ (\textbf{Algorithm})\ ,\ \Psi_{2S}(\alpha)\}\}\\
&\textbf{Stego-System}\ \Psi_{2U}\text{: } \Psi_{2U} \in \Phi_2\ \textbf{and}\\
&\Psi_{2U} = \{\ \textit{unsmooth}\ ,\ S_2^{\ U}\ ,\ \mathbf{I},\ \Psi_{2U}\ (\textbf{Algorithm})\ ,\ \Psi_{2U}(\alpha)\}\}
\end{aligned} \qquad \textbf{(29-B)}$$

$$\begin{aligned}
&\textbf{Stego-System}\ \Psi_{3S}\text{: } \Psi_{3S} \in \Phi_3\ \textbf{and}\\
&\Psi_{3S} = \{\ \textit{smooth}\ ,\ S_3^{\ S}\ ,\ \mathbf{I},\ \Psi_{3S}\ (\textbf{Algorithm})\ ,\ \Psi_{3S}(\alpha)\}\}\\
&\textbf{Stego-System}\ \Psi_{3U}\text{: } \Psi_{3U} \in \Phi_3\ \textbf{and}\\
&\Psi_{3U} = \{\ \textit{unsmooth}\ ,\ S_3^{\ U}\ ,\ \mathbf{I},\ \Psi_{3U}\ (\textbf{Algorithm})\ ,\ \Psi_{3U}(\alpha)\}\}
\end{aligned} \qquad \textbf{(29-C)}$$

Here $S_1^{\ S}$, $S_2^{\ S}$, $S_3^{\ S}$ are the three stego-images generated by using image **smooth** as Cover-image through 3 stego algorithms $\Phi_{1,}$ Φ_2 and Φ_3 respectively. using or k = 1 to 3. And $S_1^{\ U}$, $S_2^{\ U}$ and $S_3^{\ U}$ are three stego-images generated by using image **unsmooth** as Cover-image through 3 stego-algorithms $\Phi_{1,}$ Φ_2 and Φ_3 respectively.

Security of Φ_1, Φ_2 and Φ_3 ie $\Phi_1(\alpha)$, $\Phi_2(\alpha)$ and $\Phi_3(\alpha)$ is to be determined. It will be obtained by calculating the security (ε, ξ, $\bar{e}$ *and* € values) of all the six stego systems i.e. $\Psi_{1S}(\alpha)$, $\Psi_{1U}(\alpha)$, $\Psi_{2S}(\alpha)$, $\Psi_{2U}(\alpha)$, $\Psi_{3S}(\alpha)$ and $\Psi_{3U}(\alpha)$ and applying (3) on them.

Feature	Algorithm I or Φ_1(Algorithm)	Algorithm II or Φ_2(Algorithm)	Algorithm III or Φ_3(Algorithm)
Number of pixels changed if N characters are hidden in the cover image	N+1	0.3353N + 1.8096	1.534N+39.5963
Range of change in pixel values	-3 to +3	-1 to +1	Variable but ranges from -253 to +246
Data Insertion Technique	2 Bit LSB Insertion	1 Bit LSB Insertion	around 6 to 7 bits are used for data Insertion
Distribution of data in the pixel	Continuously inserts data Row by Row in every pixel right from the first row onwards. As a result the data is continuously distributed in every pixel.	Enters data in such a way that cover image and stego image remain more or less the same by pixel values having equal number of changes in +1 and -1 values so that net change in pixel value may remain close to zero.	Makes very large change in the bottom most pixels (changes in the bottom most pixel usually goes unnoticed due to psycho-visual weaknesses of human eye)
Concentration of Information in Pixel	low	Very low	Very high
Degree of Difference between the Cover Image and Stego Image (It is expressed in the scale of 1 and measured using Mean absolute Difference in the Intensity Levels of Cover and Stego Image)	0.1186	0.0671	1.00000
Degree of Changes in neighboring pixels of the pixel changed	Always Very high because it inserts data row by row.	High to Low depending on size of Cover Image	Low
Source of Algorithm	Designed in section 4 of [1]	http://quickcrypto.com/free-steganography-software.html	http://www.brothersoft.com/eureka-steganographer-v2-266233.html

Table 1 Three Different Steganographic Algorithms Used for Evaluation of Susceptibility to Steganalysis

3.1 Results

The values of $\Psi_{1S}(\alpha)$, $\Psi_{1U}(\alpha)$, $\Psi_{2S}(\alpha)$, $\Psi_{2U}(\alpha)$, $\Psi_{3S}(\alpha)$ and $\Psi_{3U}(\alpha)$ are calculated using programs in MATLAB© Image Processing Tool Box.First step for calculating the values of $\Psi_{1S}(\alpha)$, $\Psi_{1U}(\alpha)$, $\Psi_{2S}(\alpha)$, $\Psi_{2U}(\alpha)$, $\Psi_{3S}(\alpha)$ and $\Psi_{3U}(\alpha)$ is to determine the corresponding value of $\breve{e}$.

Parameters of Image (based on Section 2.2)	M = **smooth**				M = **unsmooth**			
	PIXEL	RED	GREEN	BLUE	PIXEL	RED	GREEN	BLUE
Weighted mean of the Pixel Aberration of Image M or $\delta(M)$	1.6419	2.1401	1.4854	1.3002	2.7562	2.3393	2.6980	3.2312
Max Pixel Aberration	2.2946	4.6536	3.3466	3.0648	3.8271	5.6875	5.4896	6.2048

$(\mathcal{R}(M))^{\uparrow}$								
Min Pixel Aberration $(\mathcal{R}(M))_{\downarrow}$	-1.3379	-1.2151	-2.4749	-1.4882	-1.0272	-1.5275	-1.8235	-1.6370
Range of Pixel Aberration $\mathcal{R}(M)$	3.6325	5.8688	5.8215	4.5530	4.8542	7.2150	7.3130	7.8418
Maximum Deviation in the Pixel Aberration Δ (M) and Corresponding τ given as $\mathcal{T} = \tau : \check{\tau} = \Delta$(M)	2.2946 and 7.9171	4.6536 and 12.4698	3.3466 and 9.5674	3.0648 and 8.7922	3.8271 and 11.0393	5.6875 and 14.1729	5.4896 and 13.2347	6.2048 and 15.5979
Standard Deviation of Pixel Aberrations in Image M	0.2660	0.3585	0.3294	0.3272	0.3283	0.3869	0.3991	0.3853
$\delta(M, 2)$ (as modulus of $+^{tve}$ & $-^{tve}$)	1.0675	1.5418	1.3035	1.2741	1.0269	1.1720	1.2365	1.1949
$\delta(M, 4.5)$ (as modulus of $+^{tve}$ & $-^{tve}$)	1.7062	2.3750	2.1082	1.9913	2.1402	2.7026	2.6782	2.9491
$\delta(M, 6)$ (as modulus of $+^{tve}$ & $-^{tve}$)	2.0516	2.9045	2.5827	2.4757	2.6701	3.2488	3.5855	3.7377
$\delta(M, 7.9)$ (as modulus of $+^{tve}$ & $-^{tve}$)	2.2946	3.8532	2.8856	3.0648	3.2868	4.4300	5.2156	5.3151

Table 2 Parameters (based on Section 2.2) of two test Images smooth and unsmooth

The value of $\breve{e}$ is determined by taking means of $\varepsilon(\tau)$ for τ = 0, 2, 4.5, 6 and 7.9. All these values of $\varepsilon(\tau)$ and corresponding $\breve{e}$ as well as $\grave{e}$ are given in Table 3a (for Smooth Image) and Table 3b (for Unsmooth Image). These values of $\varepsilon(\tau)$ for different τ and their average $\breve{e}$ are the measure of the difference between the pixel aberrations in the Stego-Image and the Cover-Image. Hence in order to better understand and appreciate the values of $\varepsilon(\tau)$ corresponding $\breve{e}$ and $\grave{e}$ it becomes necessary to plot the value of pixel aberration of each and every pixel (given as δ (M(z) , ℓ(M(z))) in Definiton 7 of Section 2.2) in the Cover Image and corresponding three Stego-Images (generated by the three stego-algorithms Φ_1, Φ_2 and Φ_3 operating on cover-image). As we have two different cover-images given by $\mathbb{C}$ = {**smooth**, **unsmooth**}so in Figure 2.a the pixel aberration for smooth cover-image and associated stego images are plotted whereas in Figure 2.b the pixel aberration of unsmooth cover-image and the associated stego-images are plotted. So in Figure 2.a the pixel aberration δ(M(z) , ℓ(M(z))) is plotted for M= **smooth,** S_1^S , S_2^S and S_3^S whereas in Figure 2.b the pixel aberration is plotted for M= **unmooth,** S_1^U , S_2^U and S_3^U. The various symbols used in the plot have their usual meaning. Based on the mean of the values of ε, ξ and € and $\overline{e}$ (as calculated in Table 3a and Table 3b) for all six stego-systems Ψ_{1S}, Ψ_{1U}, Ψ_{2S}, Ψ_{2U}, Ψ_{3S} and Ψ_{3U} their overall strengths given as $<\Psi_{1S}(\alpha)>$, $<\Psi_{1U}(\alpha)>$, $<\Psi_{2S}(\alpha)>$, $<\Psi_{2U}(\alpha)>$, $<\Psi_{3S}(\alpha)>$ and $<\Psi_{3U}(\alpha)>$ are calculated and shown in Table 4.

In order to better understand the values of ε, ξ the plots of relative entropy of the neighborhood (given as$H\big(P(\ell(C(z)))||P(\ell(S(z)))\big)$ in Section 2.3.1, Requirement 2) of every pixel for all the three stego-algorithms is plotted in Fig 3.a and Fig 3.b. In Fig 3.a the cover image C = ***smooth*** and Stego Image S = S_1^S , S_2^S and S_3^S where as in Fig 3.b the cover image used is C = **unmooth** and stego image S = S_1^U , S_2^U and S_3^U .

By applying (3) on these values we can conclude that:

$$\begin{aligned} <\Phi_1(\alpha)> &= \text{MAX}\ (<\Psi_{1S}(\alpha)>,\ <\Psi_{1U}(\alpha)>\ ) \\ <\Phi_2(\alpha)> &= \text{MAX}\ (<\Psi_{2S}(\alpha)>,\ <\Psi_{2U}(\alpha)>\ ) \\ <\Phi_3(\alpha)> &= \text{MAX}\ (<\Psi_{3S}(\alpha)>,\ <\Psi_{3U}(\alpha)>\ ) \end{aligned} \tag{30}$$

So

$<\Phi_1(\alpha)>$ = MAX(0.732089 , 0.524669) = 0.732089

$<\Phi_2(\alpha)>$ = MAX(0.830721 , 0.963175) = 0.963175

$<\Phi_3(\alpha)>$= MAX (5.018686, 2.560202) = 5.018686

So Algorithm 1 is most secure among all the three stego algorithms and Algorithm 3 is least secure.

Algorithm	smooth image								
	Colour	$e(0)$	$e(2)$	$e(4.5)$	$\varepsilon(6)$	$\varepsilon(7.9)$	$\breve{e}$	$\grave{e}_{MAX}$	$\grave{e}_{MEAN}$
$\Psi_{1S}(\alpha)$ (Algo)	Pixel_mean	-0.0040	-0.1738	0.0806	0.1171	0.2254	0.225255	2.1607	1.2032
	Red	-	-	0.3364	0.9711	0.8129			

		0.0080	0.1739						
	Green	-0.0032	-0.2271	-0.0021	0.0407	1.2632 xe^{-005}			
	Blue	0.0049	-0.1690	0.2956	0.6400	1.7415			
$\Psi_{2S}(\alpha)$, (QS)	Pixel_mean	0.0181	-0.1999	0.3187	0.5918	4.6908	0.792884	3.6670	1.2006
	Red	0.0491	-0.1141	0.5655	1.2580	5.7625			
	Green	0.0386	-0.1624	0.1714	0.0854	empty			
	Blue	0.0498	-0.0447	0.4032	0.7473	0.8243			
$\Psi_{3S}(\alpha)$ Eureka)	Pixel_mean	0.0303	2.1060	5.6023	6.4453	7.3028	7.794545	44.8191	38.1743
	Red	0.0351	3.1310	6.9109	8.8190	11.7963			
	Green	0.0525	5.2347	9.7561	12.9615	17.9956			
	Blue	0.0352	5.8749	12.8564	18.0777	20.8673			

Table 3.a Values of $\bar{e}$ (either $\breve{e}$ *or* $\grave{e}_{MAX\ or}\ \grave{e}_{MEAN}$) for Smooth image

Algorithm	unsmooth image								
	Colour	$e(0)$	$e(2)$	$e(4.5)$	$e(6)$	$e(7.9)$	$\breve{e}$	$\grave{e}_{MAX}$	$\grave{e}_{MEAN}$
$\Psi_{1U}(\alpha)$ (Algo)	Pixel_mean	1.1812e^{-004}	0.0042	0.0783	0.0256	0.1180	0.108875	-0.2372	0.1943
	Red	0.0012	0.0159	0.1562	0.2558	-0.1627			
	Green	0.0029	0.0294	0.3133	0.1436	-0.1053			
	Blue	0.0084	0.0965	0.5294	0.4082	0.2586			
$\Psi_{2U}(\alpha)$, (QS)	Pixel_mean	-0.0014	-7.582e^{-004}	0.0480	0.0992	-5.4725 e-^{007}	-0.004	0.7045	-0.1435
	Red	0.0033	0.0493	0.0623	0.0494	-1.5004 e^{-005}			
	Green	0.0030	0.0217	0.1678	-0.1845	-0.2026			
	Blue	0.0055	0.0151	-0.0995	0.0395	-0.0898			
$\Psi_{3U}(\alpha)$ Eureka)	Pixel_mean	0.0233	1.1202	1.8310	2.3773	3.2307	3.268105	22.1064	18.0095
	Red	0.0470	2.6542	4.8776	5.4672	6.0756			
	Green	0.0539	3.2605	5.4122	6.8352	7.7026			
	Blue	0.0439	2.6896	3.4502	4.1124	4.0975			

Table 3.b Values of $\bar{e}$ (either $\breve{e}$ *or* $\grave{e}_{MAX\ or}\ \grave{e}_{MEAN}$) for Unsmooth image

smooth image					
	ε	ξ	$\bar{e}$	€ & Color	Overall Strength
$\Psi_{1S}(\alpha)$ (Algo)	0.0294	2.2342	0.225255	0.4395 (R)	$<\Psi_{1S}(\alpha)> = 0.732089$
$\Psi_{2S}(\alpha)$, (QS)	0.0663	1.3917	0.792884	1.0720 (R)	$<\Psi_{2S}(\alpha)> = 0.830721$
$\Psi_{3S}(\alpha)$ Eureka)	0.0292	0.5931	7.794545	11.6579 (B)	$<\Psi_{3S}(\alpha)> = 5.018686$
unsmooth image					
	ε	ξ	$\bar{e}$	€ & Color	Overall Security
$\Psi_{1U}(\alpha)$	0.0425	1.8252	0.108875	-0.1221(R)	$<\Psi_{1U}(\alpha)> = 0.524669$
$\Psi_{2U}(\alpha)$	0.0313	3.8054	-0.004	-0.0120(B)	$<\Psi_{2U}(\alpha)> = 0.963175$
$\Psi_{3U}(\alpha)$	0.0086	0.9851	3.268105	3.4274 (G)	$<\Psi_{3U}(\alpha)> = 2.560202$

Table 4 Values of $\Psi_{1S}(\alpha)$, $\Psi_{1U}(\alpha)$, $\Psi_{2S}(\alpha)$, $\Psi_{2U}(\alpha)$, $\Psi_{3S}(\alpha)$ and $\Psi_{3U}(\alpha)$

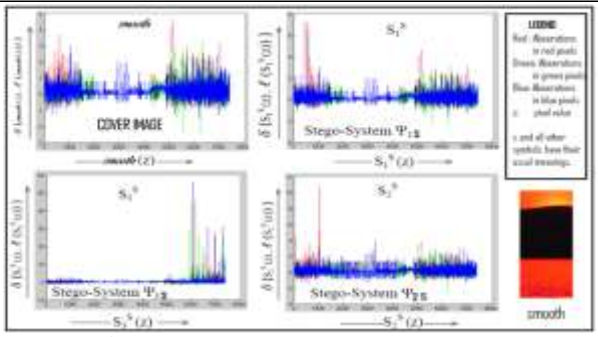

Fig 2.a Pixel Aberration plotted for Cover Image ***smooth*** and associated Stego Images S_1^S , S_2^S and S_3^S

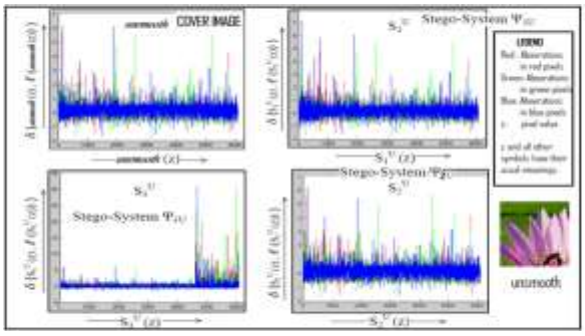

Fig 2.b Pixel Aberration plotted for Cover Image **unmooth** and associated Stego Images S_1^U , S_2^U and S_3^U

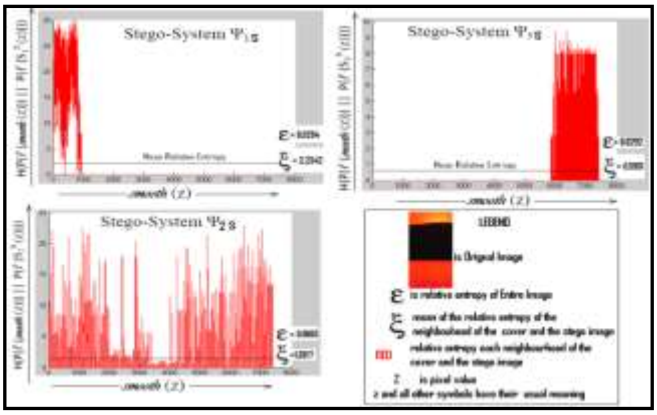

Fig 3.a Plot of Relative Entropy of neighborhood of Every Pixel in Cover Image ***smooth*** and associated Stego Images S_1^S , S_2^S and S_3^S

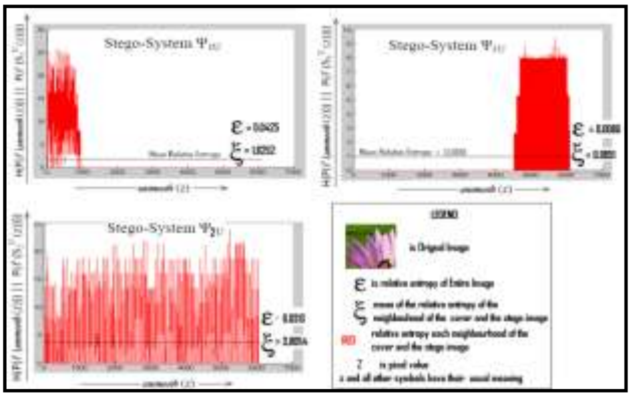

Fig 3.b Plot of Relative Entropy of neighborhood of Every Pixel in Cover Image ***unmooth*** and associated Stego Images S_1^U , S_2^U and S_3^U

3.1.1 Observations:

In Table 4 we notice that Algorithm 3 is the least secure among all three and Algorithm 1 is the most secure. Further it is interesting to note that Algorithm 2 performs better when the image is smooth where as Algorithm 1 and Algorithm 3 performs better when the image is unsmooth. In Table 3.a and Table 3.b certain values of $\varepsilon(\tau)$ are negative for certain specific τ ($\varepsilon(\tau)$ especially negative at τ =2 for Ψ_{1S} and Ψ_{2S} in Table 3.a). This indicates that when the pixel aberrations of $\tau \geq 2$ (pixels which are more than 95% deviated from the neighborhood) are considered then the cover image has more aberrations than the stego-image. In Figure 2.a we notice that although Algorithm 2 has minimum pixel aberration among

all the three but due to very high pixel aberration produced in one particular pixel (pixel aberration of more than 10 at pixel value $S_2^S(1000)$ ie at 1000th pixel) of stego image S_2^S it becomes quite susceptible to Steganalysis. Algorithm 1 performs better because it produces stego image by inserting data row by row in every pixel of cover image thus entire neighborhood of the pixel changes rendering steganlysis based on analysis of pixel aberration ineffective. Algorithm 3 has the highest pixel aberrations among all the three algorithms (clearly seen in Table 2.a and 2.b and Figure 2.a and 2.b) because it concentrates the entire information in very few pixels of bottom most row of the image. Since very few pixels are changed by Algorithm 3 so it has the minimum Relative Entropy among all the three and this is clearly conspicuous in Figure 3.a and 3.b. The graphs in Fig 3.a and 3.b are shifted Right for Algorithm 3 because it changes only the last few pixels of the cover image. From Figure 3.a and 3.b we can also conclude that Relative Entropy is highest in Algorithm 2. This is because Algorithm 2 distributes the entire information in large number of pixels as a result the probability distribution of large number of pixels changes in the stego-image (almost every pixel shows some value for relative entropy). In Algorithm 1 the graph of relative entropy (Figure 3.a and 3.b) has shifted Left and this indicates that it changes only first few pixels (exactly 900 pixels, one pixel for each character of I.

IV. Conclusion

Based on the mathematical model designed in Section 2 three different stego-algorithms were represented mathematically. Their relative strengths and weaknesses could be easily represented using the mathematical parameters and requirements defined in Section 2. Based on these mathematical parameters we can also identify any innocent looking image to be a stego image if those parameters are significantly different. Above all this model can be used for further research in Image Steganography and for representing any Image based steganographic algorithm mathematically.

V. Acknowledgement

I wish to sincerely thank Mr Kinjal Choudhary (Software Professional at Sapient Nitro), Shri D Praveen Kumar (DRDO Scientist at RCI Hyderabad), Lieutenant Mani Kumar, Sub Lieutenant S.S Niranjan (Engineering officers of Indian Navy) and Ms Anjala Sharma (Senior Engineer at Alstom Power) for keenly reviewing my work and for providing the necessary feedbacks for improvement of this technical paper. I am also thankful to entire staff of NCE in general and Shri DL Sapra (Senior Scientist, DRDO and Principal of NCE), Shri R V Kalmekar (Senior Scientist, DRDO and Vice Principal of NCE) and Commander Mohit Kaura (Senior Engineering Officer of Indian Navy and Training Commander of NCE) in particular for providing the necessary support and encouragement.

References

[1] Kaustubh Choudhary “Image Steganography and Global Terrorism” IOSR Journal of Computer Engineering, Volum 1 Issue 2 , pp 34-48.

[2] C.Cachin, “An information-theoretic model for steganography” *Proc. 2nd International Workshop Information Hiding”* LNCS 1525, pp. 306–318, 1998.

[3]. J. Zollner, H. Federrath, H. Klimant, A. Pfitzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf,“Modeling the security of steganographic systems,” *Prof. 2nd Information Hiding Workshop* , pp. 345–355,April 1998.

[4] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol. 28, pp. 656–715, Oct. 1949.

[5] Steganography Capacity: A Steganalysis Perspective R. Chandramouli and N.D. Memon

[6]. A Mathematical Approach to Steganalysis R. Chandramouli Multimedia Systems, Networking and Communications (MSyNC) Lab Department of Electrical and Computer Engineering Stevens Institute of Technology

BIBLIOGRAPHY OF AUTHOR

Kaustubh Choudhary, Scientist, Defence Research and Development Organisation (DRDO)
Ministry of Defence, Govt of India
Current attachment:
Attached with Indian Navy at Naval College of Engineering, Indian Naval Ship Shivaji,
Lonavla - 410402, Maharashtra, India