ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

Minimum Detectable Content Adaptive Steganography Using MiPOD Algorithm

[1] Ashly George, [2] Linu Babu, [3] Bency Varghese, [4] Anjali Rajan

***Abstract*— Steganography is an emerging area which is used for secured data transmission over any public media. It is a process that involves hiding a message in an appropriate carrier like image or audio. The most successful approach to steganography in digital images is to embed the payload while minimizing a suitably defined distortion function. This concept allows the stenographer to evaluate distortion caused by embedding changes based on local image content, hence the name content adaptive steganography. The sender specifies the costs of changing each cover element and then embeds a given payload by minimizing the total embedding cost. The actual embedding algorithm is realized using syndrometrellis codes to minimize the expected distortion for a given payload.**

***Keywords* – Steganography, Content adaptive, Stego, payload, cover, optimal detection**

I. INTRODUCTION

With the recent technology people are sharing more and more information among each others. Organizations fields like medicine, military are sharing data with are highly secretive and important. For secure communication people are using cryptography with the use of secret key so that only authenticate receiver can decrypt the message. But cryptography increases suspicion among attackers and tries to attack the message to get the secrete messages. A novel approach of steganography is practiced which contains a cover message embedded with secret message optionally encrypted, so that while transferring minimum suspicion arouse among attackers. But, if this approach is used by some mischievous organization then it becomes necessary to identify the stego multimedia data and try to get the information embedded in it. Like cryptanalysis which works on cryptography, Steganalysis is an art of retrieving the covert communication without affecting the cover image [7]. The primary purpose of Steganalysis is to detect the covert message and try to find more information regarding secret message length, technique of steganography used etc. [8]. The issue in steganography and Steganalysis is often modeled by the prisoner's problem [25].

A. Steganography

Steganography is the art of secret communication. In Greek, stego means covered or secret and graphy means to write and therefore, steganography becomes covered or secret writing. Its purpose is to hide the secret message, as opposed to cryp-tography, which aims to make communication unintelligible to those who dont possess the right keys [20]. We can use digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information as covers or carriers to hide secret messages [10]. After embedding a secret message into the cover image, we obtain a stego image. It is important that the stego image doesn't contain any detectable artifacts due to message embedding. A third party could use such artifacts as an indication that a secret message is present. Once a third party can reliably identify which images contain secret messages, the steganography tool becomes useless [11]. Obviously, the less information we embed into the cover image, the smaller the probability of introducing detectable artifacts by the embedding process. Important factor is the choice of the cover image. The selection is at the discretion of the person who sends the message. Images with a low number of colors, computer art, and images with unique semantic content (such as fonts) should be avoided as cover images [19]. Some steganography experts recommend grayscale images as the best cover images. They recommend uncompressed scans of photographs or images obtained with a digital camera containing a high number of colors and consider them safe for steganography [16].

B. History

Steganography has a very long history dating back many centuries. It has been used by Greeks since ancient times for secret communications. There are many stories that mention the use of secret communications in the past. One famous story is about a king who made one of his slaves shave his head, tattooed a message there and after his hair grew back, sent his slave to deliver that message without any suspicion from his opponents [25]. Similarly, there are stories about the use of wax tablets for secret communications. Wax

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

tablets were used for writing and sending messages. Many a times, to hide the message, it was written on wooden boxes, that were used to carry wax, instead of wax tablets itself and thus the message could be delivered without interception. During World War II, many invisible inks were used. Messages were written on paper with liquids like juice or urine which were normally invisible but when paper was heated, the message reappeared. Steganography techniques have been used for ages and they date back to ancient Greece [25].

The aim of stenographic communication in the past and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation the existence of hidden communication cannot be detected by third parties. What distinguishes historical stenographic methods from the modern ones is, in fact only the form of the cover (carrier) for secret data [22]. Historical methods relied on physical steganography the employed media were: human skin, etc. Further advances in hiding communication based on the use of more complex covers [19]. The popularization of the written word and the increasing literacy among people had brought about methods which used text as carrier. The World War had accelerated the development of steganography by introducing a new carrier the electromagnetic waves. Presently, the most popular carriers include digital images, audio, video files and communication protocols.

C. Basic Embedding and Extraction

Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself. There are many ways in which steganography is done. The messages appear as articles, images, lists, or sometimes invisible ink is used to write between the lines. Steganography is achieved by concealing the information in computer files. Sometimes Steganographic codes are inside the transport layer like an image file, document file, media files, etc. Due to the large size of the media files, they are considered ideal for steganography. There are three main attributes related to the information hiding; capacity, security, and robustness while using steganography, our goal is to achieve high capacity and security whereas watermarking requires high robustness.

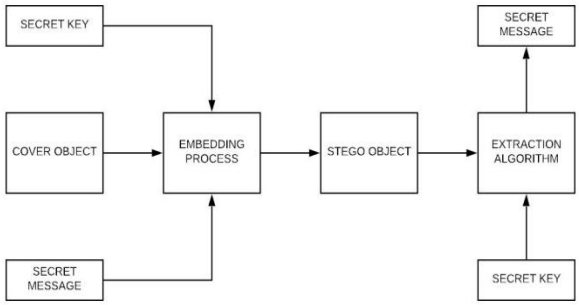

Fig. 1. Basic embedding and extraction

As shown above, secret message is embedded into the cover object by using an embedding algorithm and the resulting object is called a stego object. A stego object is one which looks exactly same as the cover object but it contains hidden information. To add more security, the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have this key. In some of these methods secret key is also used to select locations in the cover object [27].

II. MODERN STEGANOGRAPHY

With the advancement of technology in this digital age, most of the communication is carried out using some form of digital media. Similarly, it is also increasingly being used in the digital format through the use of digital media. Because of the wide spread use of internet for communication, it has become a preferable medium for digital steganography. Any digital format can be used for steganography like images, video etc., but images are still the most widely used medium and are very suitable to hide the information. There is a lot of work being done on steganography based on images as compared to other formats like audio or video, and therefore, we have mainly concentrated on the images. In the modern world of advanced cryptography, steganography is rarely used alone in important modern roles but is often combined with cryptography in communication. However, there are several areas where steganography continues to play a very important role.

Steganography is often used for uniqueness and validation purposes, such as storing data without being obvious the data is stored there. For example, almost all modern laser printers now print a series of barely visible yellow dots on every page printed. These dots, when interpreted properly, contain a variety of data about the print job, such as the date and time, printer model, and serial numbers. Stenographic messages are also commonly hidden inside of digital media often images or audio. The reason is

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

that, even if suspected, they are very hard to detect as there are plentiful different ways they could be implemented. For example, a bitmap image may have 8 bits representing each of the 3 color values (red, green, and blue) for each pixel. If we consider just the blue there will be 8 binary bits for the amount of blue in that particular pixel. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye [9]. If we modify the least significant bit (the last bit) in each byte for each color that gives of potentially hundreds of bytes of information storage and yet the overall appearance of the image will remain unchanged.

Prisoner's Problem

While considering the aspects of steganography, experts are dealing with a common example. Two stenographers, Alice and Bob, are locked in separate prison cells. They know be-forehand of their separation, so they agree on a communication strategy for planning the escape. The prisoners are allowed to send messages, however, all their communication is observed by a prison warden named Eve. If the warden finds out that they are planning to escape or even suspects so, she would cut their communication and send Alice and Bob to solitary confinement [25].

The prisoners agreed to use steganography as the mean for secret communication. The Eves approach of develop-ing statistical tests for detecting secret messages is called Steganalysis. In this scenario, the stenographic system is broken when Eve finds out that Alice and Bob are secretly communicating. In particular, the warden does not have to decode the message, which makes Steganalysis fundamentally different from cryptanalysis. Moreover, it is assumed that Eve is the passive warden the steganalyst passively monitors the channel but does not manipulate the messages. An active warden would be, for example, allowed to modify the pixels in images to destroy any potential hidden message.

III. STEGANOGRAPHIC ALGORITHMS

In general, Steganographic algorithms are divided into three types depending on the embedding domain and available information: spatial, JPEG, and side-informed JPEG. Spatial algorithms embed messages by modifying pixel values [15] while JPEG algorithms embed into quantized DCT coefficients. Side-informed algorithms utilize the knowledge of the uncompressed image and therefore the knowledge of non-quantized DCT coefficients and rounding errors. All Steganographic algorithms used in this dissertation are described below,

Spatial Domain:

- LSB matching: simple non-adaptive embedding imple-mented with ternary matric embedding.
- Edge-Adaptive (EA): This algorithm connects the embed-ding changes to pixel pairs whose difference in absolute value is as large as possible (e.g., around edges).
- HUGO: The modern content-adaptive Steganographic algorithm utilizing syndrome trellis codes. It was de-signed to minimize the embedding distortion in a high dimensional feature space computed from neighboring pixels. Its embedding simulator was run with the switch -T 255 to remove the weakness discovered during the competition.
- HUGO BD: a modification of HUGO, in which a non-additive distortion is computed only from local neigh-borhoods to allow the use of the Gibbs construction and ternary embedding.
- WOW: A highly content-adaptive scheme utilizing wavelet filter banks to evaluate the embedding distortion. Unlike HUGO, it is designed specially to avoid making embedding changes.
- S-UNIWARD: As spatial domain instance of UNIWARD distortion similar to WOW, it is wavelet-based.

A. LSB Matching and Replacement in Steganography

Many Steganographic tools are nowadays easily available on the Internet, making steganography within the reach of anyone for legitimate or malicious usage. It is thus crucial for security forces to be able to reliably detect Steganographic content among a (possibly very large) set of media files. In this operational context, the detection of rather simple but most commonly found stego system is more important than the detection of very complex but rarely encountered stego system. The vast majority of downloadable Steganographic tools insert the secret information in the LSB plane.

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image. The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same [23].

In the context of the spatial domain techniques, one of the most usual method is the LSB Replacing, where the information is embedded replacing the LSB of the pixels of the cover image. It is a variant of the LSB Replacing method, in which the pixel values will be kept unaltered in order to match correctly with respect to the hidden information, moreover, the amount of modified pixel values

are incremented or decremented by randomly manner. The Steganalysis is the counterpart of the steganography, which is used to determinate if a digital file contains hidden information or not. Recently some LSB Matching Steganalysis are proposed providing good detection rate. However, their success depends strongly on the content features of the images as well as on the image database used for evaluation. This behavior is known as inter-database error and is considered as a generalized drawback in the Steganalysis techniques for LSB Matching steganography. In order to minimize the inter database error, previous work pro-pose an image adaptive Steganalysis algorithm that considers the different content features of the images, particularly texture and plain regions[10]. In the proposed algorithm, once the input image was processed with the LSB Matching steganog-raphy method and later analyzed by a texture block classifier; the plain regions of the analyzed image are segmented from texture and edge regions. Finally, only the plain regions are considered to the Steganalysis, employing different histogram (DHCF). To determine if the image contains or not hidden information, a threshold-based decision is employed.

B. **KL Diveregence**

Steganography by cover modification can be approached from several different directions. Model-based approaches start with adopting a cover model that the embedding algorithm is forced to preserve. Although the resulting stego system is undetectable within the chosen model, such systems are de-tectable within alternative representations of the cover source. A more pragmatic approach is to admit that one will never construct a perfectly secure system for empirical objects and design the steganography to minimize a distortion function that is related to statistical detectability. Here, right from the beginning the sender gives up perfect security, and, instead, minimizes the stenographic Fisher information to maximize the size of the secure payload that can be embedded at a fixed level of statistical detectability. This approach has been extraordinarily successful and lead to practical embedding schemes that current best steganalyzers cannot reliably detect even at rather large payloads.

The most common distortion function is additive w.r.t. cover elements. The designer starts by assigning costs of changing each cover element and then embeds a given payload with the smallest possible distortion. This problem can be formulated as source coding with delity constraint [8] for which efficient near-optimal codes exist the syndrome trellis codes (STCs) [9] Freed from having to invent coding schemes for every embedding scheme, the stego designer only needs to specify the pixel costs. Non additive distortions could be made additive using the so called additive approximation by a bounding distortion [10], allowing again embedding using STCs.

C. Distortion Function

Designing Steganographic algorithms for empirical cover sources, such as digital images, is very challenging due to the fundamental lack of accurate models. The most successful approach today avoids estimating the cover source distribution because this task is infeasible for complex and highly non stationary sources. Instead, the steganography problem is formulated as source coding with fidelity constraint the sender embeds her message while minimizing an appropriately defined distortion. Practical algorithms that embed near the theoretical payload distortion bound are available for a very general class of distortion functions. Within this framework, the only task left to the sender is essentially the design of the distortion function.

All of todays most secure Steganographic schemes for digital images use heuristically defined distortion functions that constrain the embedding changes to those parts of the image that are difficult to model[3]. In the JPEG domain, by far the most successful approach is built around distortion functions that measure distortion w.r.t. the raw, uncompressed image. A natural way to define the distortion function in the spatial domain is to assign pixel costs by measuring the impact of changing each pixel in a feature space using a weighted norm. Making the weights dependent on the pixels local neighbourhood introduces desirable content adaptivity. An example of this approach is the embedding algorithm HUGO [2]. HUGO is currently the most secure algorithm for embedding in the spatial domain even though its secure payload has been substantially lowered by modern attacks.

In the spatial domain, embedding costs are typically required to be low in complex textures or noisy areas and high in smooth regions. An alternative model free approach called Wavelet Obtained Weights (WOW) uses a bank of directional high pass filters to obtain the so called directional residuals, which assess the content around each pixel along multiple different directions. By measuring the impact of embedding on every directional residual and by suitably aggregating these impacts, WOW forces the distortion to be high where the content is predictable in at least one direction and low where the content is unpredictable in every direction. The resulting algorithm is highly adaptive and has been shown to better resists Steganalysis using rich models than HUGO[21].

The distortion function proposed in this work bears similar-ity to that of WOW but is simpler and suitable for embedding in an arbitrary domain. Since the distortion is in the form of a sum of relative changes between the stego and cover images represented in the wavelet domain, hence its name universal wavelet relative distortion (UNIWARD).

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

D. **HUGO(Highly Undetectable SteGO)**

The HUGO algorithm [2] has several parameters: the range of modeled differences T, the parameters of the weight function and utilization of the model step. All these param-eters need to be set before the actual use of the algorithm. Although it can be argued that the parameters will be tied to the database, we prefer to see this step as tuning the algorithm to image source used by Alice and Bob. The security of HUGO with simulated. The HUGO algorithm [2] has several parameters: the range of modeled differences T, the parameters of the weight function λ and σ utilization of the model step. All these parameters need to be set before the actual use of the algorithm. Although it can be argued that the parameters will be tied to the database, we prefer to see this step as tuning the algorithm to image source used by Alice and Bob. The security of HUGO with simulated.

The HUGO has versions with model correction and without model correction both the algorithms may need to communicate a small number of parameters in order to able to decode the message to construct the same STC code at the receiver side. In practice, the algorithm may need to communicate a small number of parameters in order to be able to decode the message correctly. In HUGO, we need to communicate the size of the message to construct the same STC code at the receiver side. This is usually done by reserving a small portion of the image based on the stego key; where a known code is used for embedding. In HUGO algorithm, the image model was derived from SPAM features. Parts of the image model,i.e., the weights, responsible for the detection of LSB matching were identified using criteria optimized in Fisher Linear Discriminant. The coding itself was performed using the syndrome trellis codes which enable very fast implementation of the scheme in practice for arbitrary set of embedding costs ρ.

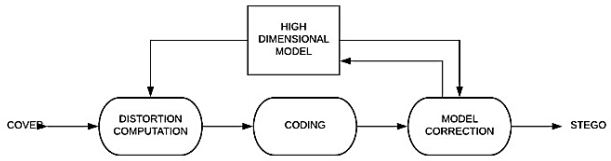

Fig. 2. High level diagram of HUGO

The design of Steganographic schemes for digital images has heavily relied on heuristic principles. The current trend calls for constraining the embedding changes to image seg-ments with complex content. Such adaptive Steganographic schemes are typically realized by first defining the cost of changing each pixel and then embedding the secret message while minimizing the sum of costs of all changed pixels. Efficient coding methods [2] can embed the desired payload with an expected distortion near the minimal possible value prescribed by the corresponding rate-distortion bound. In this work we introduce a novel type of the so-called detectability-limited sender that adjusts the payload size for each image to not exceed a prescribed level of statistical detectability within the chosen model. On a database of real images, we contrast the theoretical security of this detectability-limited sender dictated by the model. Despite the fact that the empirical detector can capture more complex dependencies between pixels than the MVG model, its detection power is much smaller. The methods of [17],[18] minimize the KL divergence between cover and stego distributions in the asymptotic limit of a small payload, while the current work minimizes the power of the most powerful detector instead of the KL divergence, which is achieved without the additional assumption of a small payload. This is why there is a new acronym MiPOD standing for Minimizing the Power of Optimal Detector[1].

IV. PROPOSED ALGORITHM

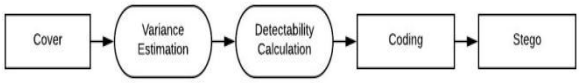

Fig. 3. Block diagram of proposed MiPOD algorithm

The goal of steganography is to communicate secret messages without revealing the very existence of the secret communication. This can be achieved by hiding the messages in inconspicuous objects. Steganography is an art of hiding information in ways that prevent the detection of hidden messages and this is achieved by hiding a piece of information inside another piece of innocent looking information. There exist a number of data embedding methods such as the spatial and time domain methods, Transform domain methods and fractal encoding methods etc. These methods hide/embed information in different types of media such as text, image, audio, video etc. Amongst these varieties of different file formats, digital images are considered to be the most popular type of carriers. A digital image is a two dimensional function f(x, y) where, x and y are spatial coordinates is the amplitude at (x,y) , also called the intensity or gray level of the image at that point and x, y, f are finite- discrete quantities. Digital Image processing is the use of computer algorithms to perform image processing on digital images. Figure 3 depicts the general block diagram of image steganography, where, at the transmitters end a secret message is embedded to an innocent looking cover image and the resultant stego image which is visually same as the original cover is then

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

transmitted over the communication channel without raising any suspicion in the minds of intermediate.

A. MiPOD Algorithm

- Estimate pixel residual variances σ_n^2 using the maximum likelihood estimator.
- Determine the change rates β_n, n = 1,….N and the Lagrange multiplier λ.
- Convert the change rates β_n to costs ρ_n.
- Embed the desired payload R using STCs with pixel costs ρ_n determined in the previous step.

B. Variance Estimation

In particular, we use a variance estimator that consists of two steps. Assuming the cover image is an 8-bit gray scale with the original pixel values z = (z_1,….z_n), $z_N \in 0,\ldots,255$, we first suppress the image content using a de-noising filter F: r = z-F(z). This can be interpreted as subtracting from each pixel its estimated expectation. The residual r will still contain some remnants of the content around edges and in complex textures. To further remove the content, and to give the estimator a modular structure that can be optimized for a given source and detector in practice, as the second step we fit a local parametric model to the neighbours of each residual value to obtain the final variance estimate. Formally, this second step of the estimator design is a block wise Maximum Likelihood Estimation (MLE) of pixel variance using a local parametric linear model [1].

Here r_n represents the values of the residual r inside the p×p block surrounding the n^{th} residual put into a column vector of size p^2×1, G is a matrix of size p^2×q that defines the parametric model of remaining expectations, a_n is a vector of q ×1 of parameters, and ξ_n is the signal whose variance we are trying to estimate. We note that ξ_n is a mixture of the acquisition noise as well as the modeling error.

Thus, our parametric model has q = $\frac{l(l+1)}{2}$ parameters, where l is the degree of the two dimensional cosine polynomial. The adaptivity of MiPOD can be adjusted by selecting different values for the parameters w, p and l. It is advantageous to use a larger block size p but keep the Wiener filter width w small. In this work, we fixed the value to w = 2. Indeed, pixels with $\sigma_n^2 \approx 0$ lie in a smooth image region and should have a small probability of change anyway. In practice, for numerical stability, we introduce a finite floor for the estimated variance.

C. Change Rate Estimation

Maximizing the security under the omniscient Warden means that Alice should select change rates β_n that minimize the deflection coefficient under the payload constraint. This can be easily established using the method of Lagrange multipliers. The change rates β_n and the Lagrange multiplier λ>0 that minimizes the deflection coefficient must satisfy the following N +1 non-linear equations for N+1 unknowns, which are and the change rates $\beta_1,\ldots,\beta_N$.

Fisher information improves MiPODs security by smoothing it and in MiPOD, the linear parametric model is applied pixel wise, which makes variance estimations of neighboring pixels (and the associated pixel costs) strongly correlated. H(x)= -2xlogx-(1-2x)log(1-2x) is the ternary entropy function expressed in nats ("log" is the natural log). In practice, Alice needs to use some coding method, such as the syndrome-trellis codes (STCs) [24].

D. Cost Estimation

Once the change rates are computed, they need to be converted to costs so that the actual message embedding can be executed with the well-established framework of syndrome-trellis codes. The costs can be obtained by inverting the relationship between β_n and ρ_n.

$$\rho_n = ln\frac{1}{(\beta_n - 2)} \qquad (1)$$

V. CONCLUSION

We introduced a novel method for steganography by minimizing the statistical detectability. This method presented a technique for Image steganography based on minimizing the power of an optimal detector. The approach specified the cost of changing each cover element, and then embedded the payload by minimizing the total embedding cost. What makes our proposed approach different is that the fact that it do not attempt to preserve the model but rather minimize the impact of embedding. By adjusting the parameters of the model variance estimator, the embedding scheme called MiPOD gives the security of the most advanced Steganographic schemes. This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner.

Fig. 4. Cover and Stego images

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

The figure 4 represents the cover image, in which the payload is embedded. It is a gray scale image of pixel size 512×512. We removed the noise from the cover image by using a two dimensional Wiener filter with size [2,2]. The variance is estimated using Maximum Likelihood Estimator and the pixel wise variance is obtained. Fisher information is calculated from the estimated variance. Embedding procedure is done by minimizing the cost. Change rate is calculated using iterative procedure. It is converted into cost term.

The secret data is embedded on the cover image. The resulted image is known as stego image, which is also a gray scale image of same size as that of the cover image as shown in figure 5. Both the cover and stego image are looking same; also it is evident that the detectability is minimized. A third party cannot recognize that the image contain a hidden information. By calculating the probability of error for different cover images, the error may differ. But the difference is very small. So the detectability is minimum.

APPENDIX A

IMAGE MODEL

A. Cover image model

Formally, we consider the cover pixels as an N dimensional vector z = (z_1,….,z_N) of independent realizations of N Gaussian random variables Z_N ~N(μ_n,ω_n^2), n = 1,…,N, quantized to discrete points kΔ, kϵZ (for simplicity and without loss on generality, we set Δ= 1). Here, μ_n is the noise-free content and ω_n^2 the variance of the Gaussian acquisition noise. Let μ_n^2 be an estimate of the mean of the n^{th} pixel. The differences $x_n = z_n - \mu_n$ will thus contain both the acquisition noise as well as the modeling error. We model x_n as independent Gaussian random variable X_n ~N(0,σ_n^2), where $\sigma_n^2 \geq \omega_n{}^2$ because of the inclusion of the modeling error.

Assuming the fine quantization limit, Δ<<σ_n for all n , the probability mass function (pmf) of the n^{th} pixel is given by $P\sigma_n = (P\sigma_n(k))_{k\epsilon Z}$ with

$$P\sigma_n(k) = P(x_n = k)\ \alpha \frac{1}{\sigma n 2\prod} \exp\ \frac{-k\hat{}2}{2\sigma_n^2} \qquad (2)$$

B. Stego image model

A widely adopted and well-studied model of data hiding is the Mutually Independent(MI) embedding in which the embedding changes Alice makes at each pixel are independent of each other. In particular, we adopt one of the simplest possible setups when the pixel values are changed by at most ±1 (the so-called LSB matching or LSBM) while noting that the framework is easily extensible to any MI embedding. Given a cover image represented with x = (x_1,…., x_N), the stego image y = (y_1,….,y_N) is obtained by independently applying the following probabilistic rules

$$P(y_n = x_n + 1) = \beta_n$$
$$P(y_n = x_n - 1) = \beta_n$$
$$P(y_n = x_n) = 1 - 2\beta n \qquad (3)$$

with change rates 0 ≤ βn ≤ 1/3

$$D(x,y) = \sum_{n=1}^{N} \rho_{n[x_n \neq y_n]} \qquad (5)$$

Where, $\rho_n \geq 0$ is the cost of changing pixel x_n tied to β_n via

$$\beta_n = \frac{e^{(-\lambda\rho_n)}}{1 + 2e^{-\lambda\rho_n}} \qquad (6)$$

with λ>0 determined from the payload constraint (4).

C. Embedding in practice

In theory, if Alice used an optimal embedding scheme, she could embed a payload of R nats:

$$R(\beta) = X \sum_{n=1}^{N} H(\beta_n) \qquad (4)$$

Where H(x) = −2xlogx−(1−2x)log(1−2x) is the ternary entropy function expressed in nats (log is the natural log). In practice, Alice needs to use some coding method, such as the syndrome-trellis codes (STCs) [2] while minimizing the following additive distortion function

$$D(x,y) = \sum_{n=1}^{N} \rho_{n[x_n \neq y_n]} \qquad (5)$$

Where, $\rho_n \geq 0$ is the cost of changing pixel x_n tied to β_n via

$$\beta_n = \frac{e^{-\lambda\rho_n}}{1 + 2e^{(-\lambda\rho_n)}} \qquad (6)$$

with λ>0 determined from the payload constraint (4)

D. Estimating pixel variance

In particular, we use a variance estimator that consists of two steps. Assuming the cover image is an 8-bit gray scale with the original pixel values z = $(z_1, \ldots, z_N)$, zn∈ 0, ..., 255, we first suppress the image content using a de-noising filter F : r = z −F(z). This can be interpreted as subtracting from each pixel its estimated expectation. The residual r will still contain some remnants of the content around edges and in complex textures. To further remove the content, and to give the estimator a modular structure that can be optimized for a given source and detector in practice, as the second step we fit a local parametric model to the neighbours of

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

each residual value to obtain the final variance estimate.

Formally, this second step of the estimator design is a block wise Maximum Likelihood Estimation(MLE) of pixel variance using a local parametric linear model. We model the remaining pixel expectation within small p × p blocks as follows:

$$r_n = Ga_n + \xi_n \qquad (7)$$

Here $r_n$represents the values of the residual r inside the p × p block surrounding the n th residual put into a column vector of size $P^2 \times 1$, G is a matrix of size $P^2 \times q$ that defines the parametric model of remaining expectations, an is a vector of q × 1 of parameters, and ξ_n is the signal whose variance we are trying to estimate. We note that ξ_n is a mixture of the acquisition noise as well as the modelling error.

It is well known that for a linear model corrupted by Gaussian noise, the MLE of the parameter an from the residuals rn is given by:

$$\hat{a}(n) = (G^T G)^{-1} G^T r_n \qquad (8)$$

Hence, the estimated expectation of the residuals rn is given by:

$$\check{r}_n = G\hat{a}(n) = G(G^T G)^{-1} G^T r_n \qquad (9)$$

Finally, assuming that the pixels within the n th block have the same or similar variances, from (23) the MLE estimation of the central pixel variance in the n th block is:

$$\sigma_{n^2} = \frac{\|P \perp G r_n\|^2}{P^2 - q} \qquad (10)$$

Where, $P \perp G = I_n - G(G^T G)^{-1} G^T$ represents the orthogonal projection onto the $P^2 \times 1$ dimensional subspace spanned by the left null space of G (I_n is the n × n unity matrix).

Thus, our parametric model has q = l(l + 1)/2 parameters, where l is the degree of the two dimensional cosine polynomial

The adaptivity of MiPOD can be adjusted by selecting different values for the parameters w, p and l. It is advantageous to use a larger block size p but keep the Wiener filter width w small.

Indeed, pixels with $\hat{\sigma}_n^2 \approx 0$ lie in a smooth image region and should have a small probability of change anyway. In practice, for numerical stability, we introduce a finite floor for the estimated variance:

$$\hat{\sigma}_n^2 \leftarrow \max(0.01, \hat{\sigma}_n^2).$$

REFERENCES

[1] Vahid Sedighi, Remi Cogranne, Jessica Fridrich ”Content-Adaptive Steganography by Minimizing Statistical Detectability” IEEE Transactions on Information Forensics and Security, vol.11, Issue.2, pp.1-14, February 2016.

[2] T. Pevny, T. Filler, and P. Bas, Using high-dimensional image models to perform highly undetectable steganography Information Hiding,12th International Conference, vol.6387 of LNCS, (Calgary, Canada), pp.161177, Springer-Verlag, New York, June 2830, 2010.

[3] V. Holub and J. Fridrich, Designing steganographic distortion using directional filters, Proc. IEEE WIFS, (Tenerife, Spain), December 25, 2012.

[4] V. Holub, J. Fridrich, and T. Denemark, Universal distortion design for steganography in an arbitrary domain, EURASIP Journal on Information Security, Special Issue on Revised Selected Papers of the 1st ACM IH and MMS Workshop, vol.1, 2014.

[5] B. Li, M. Wang, and J. Huang, A new cost function for spatial image steganography, Proceedings IEEE ICIP, (Paris, France), October 2730, 2014.

[6] B. Li, S. Tan, M. Wang, and J. Huang, Investigation on cost assignment in spatial image steganography, IEEE TIFS,vol.9, pp.12641277, August 2014.

[7] R.Bohme, Advanced Statistical Steganalysis, Berlin Heidel berg: Springer-Verlag, 2010.

[8] A. D. Ker, P. Bas, R. Bohme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevn, Moving steganography and steganalysis from the laboratory into the real world, 1st ACM IH MMSec.Workshop (W.Puech,M.Chaumont,J.Dittmann, and P. Campisi, eds.), (Montpellier, France), June 1719, 2013.

[9] T. Pevn, P. Bas, and J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, IEEE TIFS, vol.5, pp.215224, June 2010.

[10] T. Filler and J. Fridrich, Design of adaptive steganographic schemes for digital images, Proceedings SPIE, Electronic Imaging, Media Watermarking, Security and Forensics III (A. Alattar, N. D. Memon, E. J. Delp, and J. Dittmann, eds.), vol.7880, (San Francisco, CA), pp.114, January 2326, 2011.

[11] R. J. Anderson and F.A.P. Pettitcolas ”On the limits of steganography” IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, pp. 474-481, 1998.

[12] J. Fridrich, M. Goljan, and R. Du, (2001) ”Detecting LSB steganography in color, and gray-scale images” Multimedia, IEEEVOL.4,NO.4.

[13] J. Fridrich, J. Kodovsk, M. Goljan, and V. Holub ”Breaking HUGO The process discovery” in Proc. 13th Int. Conf., May 2011, pp.85101.

[14] P. Bas, T. Filler, and T. Pevn ”Break our steganographic systemThe ins and outs of organizing BOSS” in Proc. 13th Int. Conf., May 2011, pp.5970.

[15] J. Fridrich, J. Kodovsk, M. Goljan, and V. Holub ”Steganalysis of content-adaptive steganography in

spatial domain" in Proc. 13th Int. Conf., May 2011, pp.102117.

[16] J. Kodovsk, J. Fridrich, and V. Holub, On dangers of overtraining steganography to incomplete cover model, Proceedings of the 13th ACM Multimedia Security Workshop, Niagara Falls, NY), pp.6976, September 2930, 2011.

[17] Fridrich and J. Kodovsk, Multivariate Gaussian model for designing additive distortion for steganography, in Proc. IEEE ICASSP, (Vancouver, BC), May 2631, 2013.

[18] V. Sedighi, J. Fridrich, and R. Cogranne, Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model, in Proceedings SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics 2015, (San Francisco, CA), February 911, 2015.

[19] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu, A cover image model for reliable steganalysis, in Information Hiding,13th International Conference,vol.7692 of LNCS, (Prague, Czech Republic), pp.178192, May 1820, 2011.

[20] J. Fridrich and J. Kodovsk, Rich models for steganalysis of digital images, IEEE TIFS, vol.7, pp.868882, June 2011.

[21] W. Tang, H. Li, W. Luo, and J. Huang, Adaptive steganalysis against WOW embedding algorithm, in 2nd ACMIHMMSec. Workshop, (Salzburg, Austria), June 1113, 2014.

[22] A. D. Ker, Batch steganography and pooled steganalysis, in Information Hiding, 8th International Workshop (J. L. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, eds.), vol.4437 of LNCS, (Alexandria, VA), pp.265281, Springer Verlag, New York, July 1012, 2006.

[23] Oswaldo Juarez-Sandoval, Manuel Cedillo-Hernandez, Mariko Nakano-Miyatake, Hector Perez-Meana,and Karina Toscano-Medina, Image-Adaptive Steganalysis for LSB Matching Steganography, in Proc. SPIE Security Watermarking Multimedia Contents, vol.4675,2016.

[24] Tom Filler, Jan Judas, and Jessica Fridrich, "Minimizing Additive Dis-tortion in Steganography using Syndrome-Trellis Codes," in Information Hiding, 8th International Workshop.

[25] Vojtech Holub, Content adaptive steganography design and detection PhD thesis dissertion 2014

[26] Jan Kodovsk, Jessica Fridrich On Completeness of Feature Spaces in Blind Steganalysis,

[27] Mamta juneja,Parvinder Singh Sandhu Improved information security using Steganography and Image Segmentation during transmission,

[28] V.Gokula Krishanan, M.Deepak, S.Praveen Kumar, B.Vinoth Kumar "Statistical Stegnalaysis for Content-Adaptive Steganography," Inter-national Journal of Engineering Science and Computing, March 2016.