2018

Information Hiding Using Convolutional Encoding

Jonathan Blackledge
Technological University Dublin, jonathan.blackledge@tudublin.ie

Paul Tobin
Technological University Dublin, paul.tobin@tudublin.ie

J. Myeza
University of KwaZulu-Natal, myezaj3@ukzn.ac.za

C. M. Adolfo
Military Technological College, Muscat, Oman, cidmathew.adolfo1@gmail.com

Recommended Citation
Blackledge, J.M., Tobin, P., Myeza, J. & C.M. Adolfo. (2018). Information hiding using convolutional encoding. *ISSC 2018: 29th. Irish Signals and Systems Conference*. Queen's University Belfast, Northern Ireland, 21-22 June.

Information Hiding using Convolutional Encoding

J. M. Blackledge
Stokes Professor, Science Foundation Ireland
Honorary Professor, Dublin Institute of Technology
Professor Extraordinaire, University of Western Cape
jonathan.blackledge@dit.ie

P. Tobin
Department of Electrical and Electronic Engineering
Dublin Institute of Technology
Dublin, Ireland.
paul.tobin@dit.ie

J. Myeza
Department of Information Systems and Technology
University of KwaZulu-Natal
Durban, South Africa.
Myezaj3@ukzn.ac.za

C. M. Adolfo
Department of Systems Engineering
Military Technological College
Muscat, Oman.
cidmathew.adolfo1@gmail.com

***Abstract*—We consider two functions $f_1(\mathbf{r})$ and $f_2(\mathbf{r})$, for $\mathbf{r} \in \mathbb{R}^n$ and the problem of 'Diffusing' these functions together, followed by the application of an encryption process we call 'Stochastic Diffusion' and then hiding the output of this process in to one or other of the same functions. The coupling of these two processes (i.e., data diffusion and stochastic diffusion) is considered using a form of conditioning that generates a well-posed and data consistent inverse solution for the purpose of decrypting the output.**

After presenting the basic encryption method and (encrypted) information hiding model, coupled with a mathematical analysis (within the context of 'convolutional encoding'), we provide a case study which is concerned with the implementation of the approach for full-colour 24-bit digital images. The ideas considered yields the foundations for a number of wide-ranging applications that include covert signal and image information interchange, data authentication, copyright protection and digital rights management, for example.

***Index Terms*—Encryption, Steganography, Steganocryptography, Information Hiding, Data Diffusion, Stochastic Diffusion.**

I. Introduction

The development of techniques for hiding information [1], and, in particular, the field of Steganography, is important in situations when encryption cannot assure data security due to the encrypted information arousing suspicion or when the transmission of encrypted information is incriminating (e.g. in situations when the transmission of encrypted information is banned, is illegal or subject to investigatory powers [2]). Information hiding techniques generally embed plaintext data into covertext data that one wishes to send secretly via an innocuous 'message' based on the transmission of so-called stegotext data, which should be in a form that restricts detection or recovery of the hidden data. There are two principal data hiding categories, namely, Watermarking and Steganography, [3] and [4]. The work reported in this paper is based on the latter case coupled with a further restriction on the recovery of hidden data which is to first encrypt the data before hiding it, an approach that we refer to as Steganocryptography [5].

978-1-5386-6046-/18/$31.00 © 2018 IEEE

The information hiding method reported here considers a convolutional encoding based approach which involves two principal processes, namely, 'Data Diffusion' and 'Stochastic Diffusion', the latter method having been researched and implemented in a number of previous publications, e.g. [6], [7], [8], and [9]. These processes are used to develop a highly fragile and thereby tamper-proof method of hiding encrypted data in a host data field. The method utilises the properties and characteristics of the Fourier transformation and the convolution and correlation integrals, and developed for arbitrary dimensions so that applications of the method can be used for encrypting and hiding information in digital signals, digital images and for three-and four-dimensional (i.e., three-dimensions + time) signal processing applications. We consider a case study that focuses on encrypted full-colour image information hiding with applications that can include image and e-document authentication, copyright protection and covert encryption. To the best of the author's knowledge, the approach considered in this paper and the application reported in the Case Study (Section V), is new and original, specifically, the coupling of the data diffusion and stochastic diffusion processes to produce an encryption scheme whose inverse is ill-posed in absence of the covertext, much of the paper being based on the material reported previously in [10].

II. Convolutional Coding Revisited

Given a binary input stream $f[n] = \{0,1\}^\ell$ consisting of a 'block length' of ℓ bits (0 or 1), for a binary Finite Impulse Response function $g[n]$ say, a convolutional encoder yields an encoded output $h^\ell[n]$ given by [11]

$$h^\ell[n] = \sum_m g[n-m] f^\ell[m]$$

A convolutional encoder of this type describes a discrete linear time-invariant system which is a fundamental model for

processing digital signals in general, when $f[n]$, $g[n]$ and $h[n]$ may be integer or floating point arrays.

Convolutional codes are used extensively to achieve reliable data transfer in numerous applications, such as digital video, radio, mobile communications and satellite communications [12]. These codes are often implemented in concatenation with a hard-decision code, and, prior to turbo codes, such constructions were the most efficient, coming closest to the Shannon limit. One of the principal reason for using convolutional encoding is that maximum-likelihood decoding can be achieved with reasonable complexity using time-invariant trellis based decoders - the 'Viterbi algorithm' [13], for example, being a common example of such an 'error correction code' [14]. In this context, we consider an approach that is based on extending the convolutional encoding process to data fields of arbitrary dimensions while considering a modification to the process that yields a well-posed inverse solution to the decoding (deconvolution) problem.

Consider a function $f(\mathbf{r})$ for $\mathbf{r} \in \mathbb{R}^n$ with n-dimensional Fourier and inverse Fourier transforms

$$F(\mathbf{k}) = \mathcal{F}_n[f(\mathbf{r})] \equiv \int_{-\infty}^{\infty} f(\mathbf{r}) \exp(-i\mathbf{k}\cdot\mathbf{r}) d^n\mathbf{r} \text{ and}$$

$$f(\mathbf{r}) = \mathcal{F}_n^{-1}[F(\mathbf{k})] \equiv \frac{1}{(2\pi)^n} \int_{-\infty}^{\infty} F(\mathbf{k}) \exp(i\mathbf{k}\cdot\mathbf{r}) d^n\mathbf{k}$$

respectively, $\mathbf{k}$ being the spatial frequency vector. If $g(\mathbf{r})$ is some stochastic function (a cipher) generated by a known algorithm or some other source (a 'code' or natural noise, for example), then convolutional encoding involves convolving $g(\mathbf{r})$ with $f(\mathbf{r})$ to produce an output $h(\mathbf{r})$ say, which we can write as ($\otimes$ denoting the n^{th} order convolution integral $\forall \mathbf{r} \in \mathbb{R}^n$)

$$h(\mathbf{r}) = g(\mathbf{r}) \otimes f(\mathbf{r}) \equiv \int_{-\infty}^{\infty} g(\mathbf{r}-\mathbf{r}') f(\mathbf{r}') d^n\mathbf{r}'$$

The transmission of such an output is taken to be corrupted by additive transmission noise described by the function $n(\mathbf{r})$, say, which introduces errors into the recovery of $f(\mathbf{r})$ from $h(\mathbf{r})$ and thus we arrive at an equation of the form

$$h(\mathbf{r}) = g(\mathbf{r}) \otimes f(\mathbf{r}) + n(\mathbf{r}) \tag{1}$$

under the assumption that

$$\|n(\mathbf{r})\| << \|g(\mathbf{r}) \otimes f(\mathbf{r})\| \leq \|g(\mathbf{r})\| \times \|f(\mathbf{r})\|$$

the ratio $\|g(\mathbf{r}) \otimes f(\mathbf{r})\| / \|n(\mathbf{r})\|$ being known, in general, as the Signal-to-Noise Ratio or SNR in the fields of signal processing when $\mathbf{r} \in \mathbb{R}^1$ and image processing when $\mathbf{r} \in \mathbb{R}^2$.

This inverse (deconvolution) problem is as follows: Given equation (1), and, with functions $h(\mathbf{r})$ and $g(\mathbf{r})$ known, obtain a solution for $f(\mathbf{r})$. In some cases, $g(\mathbf{r})$ may not be known and the problem becomes the so-called 'blind deconvolution problem'. In general, this problem is an ill-posed problem, and consequently, has a range of solutions whose purpose is usually to regularise the inverse solution in such a way that an optimum estimate of $f(\mathbf{r})$ can be obtained subject to certain conditions. Most such solutions take the form $\hat{f}(\mathbf{r}) = q(\mathbf{r}) \otimes h(\mathbf{r})$ where $\hat{f}(\mathbf{r})$ is an estimate of $f(\mathbf{r})$, $q(\mathbf{r})$ is some filter with Fourier transform $Q(\mathbf{k}) = \mathcal{F}_n[q(\mathbf{r})]$.

The nature of equation (1) and the conventional (discrete) convolutional encoding/decoding processes as discussed in this section, is based on a model for an n-dimensional signal that is ultimately related to the physical process that leads to the generation and detection of a signal, [16], [17]. Equation (1) is thus taken to be a fundamental model for the analysis and processing of signals in general (albeit for the linear and time or space invariant case) in a multitude of signal and image processing applications, and, for this reason, solutions to the deconvolution problem have been studied widely, e.g., [15] and [17] and references therein. However, in regard to the development of data encryption methods, we are at liberty to 'invent' ideas that do not necessarily need to conform to a systems model derived from and constrained by physical principles (excluding the field of quantum cryptography). In this context, the foundations for the approach considered in this paper are compounded in the following section.

III. Well-posed Deconvolution

The ill-posed nature of the deconvolution problem compounded in equation (1) can lead to issues in the practical use of convolutional encoding in terms of providing a unique solution without the need to utilise error correction schemes and/or regularisation techniques as briefly discussed in the previous section. We now consider a fundamental theorem associated with solving the deconvolution problem by 'designing' a problem that is well-posed.

The 'key' to the original theme developed in this paper and applications thereof is compounded in the following result: For $\mathbf{r} \in \mathbb{R}^n$ given the equation,

$$h(\mathbf{r}) \otimes [g^*(\mathbf{r}) \odot g(\mathbf{r})] = f(\mathbf{r}) \otimes g(\mathbf{r}) \tag{2}$$

where $h(\mathbf{r})$ and $g(\mathbf{r})$ are known (real or complex) functions ($\otimes$, $\odot$ and * denoting the n^{th}-order convolution integral, correlation integral and complex conjugate, respectively), the exact solution for $f(\mathbf{r})$ is given by

$$f(\mathbf{r}) = g^*(\mathbf{r}) \odot h(\mathbf{r}) \tag{3}$$

This result is easily derived by using the convolution and correlation theorems so that equation (2) can be written in Fourier space as

$$H(\mathbf{k}) \mid G(\mathbf{k}) \mid^2 = F(\mathbf{k}) G(\mathbf{k})$$

Multiplying both sides of this equation by $G^*(\mathbf{k})$ we obtain

$$F(\mathbf{k}) = G^*(\mathbf{k}) H(\mathbf{k})$$

and using the correlation theorem, equation (3) is obtained. Note that the solution for $f(\mathbf{r})$ does not rely on the condition $\mid G(\mathbf{k}) \mid^2 > 0 \ \forall \mathbf{k}$ (as is the case with the generalised

deconvolution problem if regularisation is not imposed) and is therefore a well-posed solution.

Equation (2) is consistent with an Infinite Impulse Response (IIR) filter model (which is common in the presence of a feedback topology) for a 'perfect feedforward filter'. The argument for this is as follows: For $\mathbf{r} \in \mathbb{R}^n$ the output from a IIR filter is given by

$$h(\mathbf{r}) = g(\mathbf{r}) \otimes f(\mathbf{r}) - p(\mathbf{r}) \otimes h(\mathbf{r})$$

where $g(\mathbf{r})$ denotes the feedforward filter function and $p(\mathbf{r})$ denotes the feedback filter function. Fourier transformation shows that

$$H(\mathbf{k}) = \frac{G(\mathbf{k})Q^*(\mathbf{k})}{\mid Q(\mathbf{k}) \mid^2} F(\mathbf{k}),\ Q(\mathbf{k}) = 1 + P(\mathbf{k})$$

so that upon rearrangement and inverse Fourier transformation we obtain

$$h(\mathbf{r}) \otimes [q^*(\mathbf{r}) \odot q(\mathbf{r})] = g(\mathbf{r}) \otimes [q^*(\mathbf{r}) \odot f(\mathbf{r})]$$

Thus, in the case when the feedforward filter is a perfect filter, i.e., when $g(\mathbf{r}) = \delta^n(\mathbf{r})$, then

$$h(\mathbf{r}) \otimes [q^*(\mathbf{r}) \odot q(\mathbf{r})] = q^*(\mathbf{r}) \odot f(\mathbf{r})$$

and it is clear that $f(\mathbf{r})$ can be recovered from $h(\mathbf{r})$ by convolution with the feedback filter function.

IV. Encrypted Information Hiding

Consider two functions $f_1(\mathbf{r})$ and $f_2(\mathbf{r})$ and the problem of how to hide an encrypted form of the function $f_1(\mathbf{r})$ (using convolutional encoding) by embedding it in the function $f_2(\mathbf{r})$ (or vice versa as required). The problem falls into the field *Steganocryptography*, cryptography being concerned with the encryption of information and steganography being concerned with the 'art' of hiding the content of one message in another. Here, we are interested in hiding encrypted information (a ciphertext in a covertext to produce an output known as a stegotext).

A. Data Hiding and Recovery

Ignoring the encryption process (for the moment), consider the case when

$$\|f_1(\mathbf{r})\|_\infty = 1 \text{ and } \|f_2(\mathbf{r})\|_\infty = 1$$

where

$$\|f(\mathbf{r})\|_\infty \equiv \sup\{\mid f(\mathbf{r}) \mid : \mathbf{r} \in \mathbb{R}^n\}$$

and the additive 'information embedding equation'

$$h(\mathbf{r}) = cf_1(\mathbf{r}) + f_2(\mathbf{r}),\ c \in [0, 1]$$

where the constant c is the 'Information Embedding Coefficient' (IEC). In this context, $f_2(\mathbf{r})$ is referred to as the covertext, $h(\mathbf{r})$ is referred to as the stegotext, $f_1(\mathbf{r})$ is referred to as the plaintext, and, in order to hide the function $f_1(\mathbf{r})$ in $f_2(\mathbf{r})$ effectively, we require that $c\|f_1(\mathbf{r})\| << \|f_2(\mathbf{r})\|$.

Clearly, given that $\|f_1(\mathbf{r})\|_\infty = 1$ and $\|f_2(\mathbf{r})\|_\infty = 1$, the smaller the value of c, the smaller the perturbation of $f_1(\mathbf{r})$ to $f_2(\mathbf{r})$ becomes, and, in practical applications of the approach being considered here, necessitates optimization in such a way that c is a minimum subject to the optimal reconstruction of $f_1(\mathbf{r})$ through application of the equation

$$f_1(\mathbf{r}) = \frac{1}{c}[h(\mathbf{r}) - f_2(\mathbf{r})]$$

We can also apply an information hiding strategy based on any exactly invertible transformation, e.g.,

$$h(\mathbf{r}) = \mathcal{F}_n^{-1}[cF_1(\mathbf{k}) + F_2(\mathbf{k})]$$

where $F_1(\mathbf{k}) = \mathcal{F}_n[f_1(\mathbf{r})],\ \ F_2(\mathbf{k}) = \mathcal{F}_n[f_2(\mathbf{r})]$ and

$$f_1(\mathbf{r}) = \frac{1}{c}\mathcal{F}_n^{-1}[H(\mathbf{k}) - F_2(\mathbf{k})],\ H(\mathbf{k}) = \mathcal{F}_n[h(\mathbf{r})]$$

Also, note that since $\|f_1(\mathbf{r})\|_\infty = 1$, renormalisation can be applied in the computation of $f_1(\mathbf{r})$ thereby eliminating the need to apply a multiplication by $1/c$, i.e., we can consider the equation

$$f_1(\mathbf{r}) = \frac{\mathcal{F}_n^{-1}[H(\mathbf{k}) - F_2(\mathbf{k})]}{\|\mathcal{F}_n^{-1}[H(\mathbf{k}) - F_2(\mathbf{k})]\|_\infty}$$

which avoids the need to know the precise value of c in the recovery of the hidden data $f_1(\mathbf{r})$.

B. Data Diffusion

In order to recover the function $f_1(\mathbf{r})$ from $h(\mathbf{r})$ it is clear that $f_2(\mathbf{r})$ - the covertext - must be known. Because of this, we consider the process of 'diffusing' the two function $f_1(\mathbf{r})$ and $f_2(\mathbf{r})$ using convolutional encoding based on the properties of equation (2). Thus, consider the construction of the function

$$g(\mathbf{r}) = \mathcal{F}_n^{-1}\left[\frac{F_2(\mathbf{k})F_1(\mathbf{k})}{\mid F_2(\mathbf{k}) \mid^2}\right]$$

under the condition that if the power spectrum $\mid F_2(\mathbf{k}) \mid^2 = 0$ for any value of $\mathbf{k}$, then it is set to a value of 1 in order to avoid any singularities that may occur in the computation of the inverse filter $F_2(\mathbf{k})/ \mid F_2(\mathbf{k}) \mid^2$ given that in any and all cases, when $F_2(\mathbf{k}) = 0$, we can apply the conditional result: $F_2(\mathbf{k})/ \mid F_2(\mathbf{k}) \mid^2 = F_2(\mathbf{k}) = 0$. Subject to this 'renormalisation condition', from Theorem 3.1, it is clear that $f_1(\mathbf{r})$ can be recovered from $g(\mathbf{r})$ by correlating $g(\mathbf{r})$ with $f_2^*(\mathbf{r})$. If we then apply the Fourier-based hiding method discussed in the previous section, then we can hide the function $g(\mathbf{r})$ in the covertext function f_2 to construct the stegotext function as follows:

$$h(\mathbf{r}) = F_n^{-1}[cG(\mathbf{k}) + F_2(\mathbf{k})],\ G(\mathbf{k}) = \mathcal{F}_n[g(\mathbf{r})],\ c \in [0, 1]$$

C. Stochastic Diffusion

In addition to applying data diffusion, we can go further and diffuse the function $g(\mathbf{r})$ with a stochastic function $s(\mathbf{r})$, say, which in practice, is taken to be generated by applying some key-dependent (cryptographically-strong) random number generating algorithm (with a uniform statistical distribution, a uniform power spectral density function, a high Lyapunov exponent and high cycle length, for example).

We call this process 'Stochastic Diffusion' and is based on constructing the function

$$v(\mathbf{r}) = \mathcal{F}_n^{-1}\left[\frac{S(\mathbf{k})G(\mathbf{k})}{\mid S(\mathbf{k}) \mid^2}\right]$$

subject to the same re-normalisation condition as discussed Section III. We can then construct the following stegotext function

$$h(\mathbf{r}) = \mathcal{F}_n^{-1}[cV(\mathbf{k}) + F_2(\mathbf{k})],\ V(\mathbf{k}) = \mathcal{F}_n[v(\mathbf{r})],\ c \in [0,1]$$

in the knowledge that, via Theorem 3.1, $f_1(\mathbf{r})$ can be recovered by correlating $v(\mathbf{r})$ with $s^*(\mathbf{r})$ to obtained $g(\mathbf{r})$ and then correlating $g(\mathbf{r})$ with $f_2^*(\mathbf{r})$ to recover the plaintext $f_1(\mathbf{r})$. Note that this process can be repeated, i.e. $v_1(\mathbf{r}) \equiv v(\mathbf{r})$ can be diffused with another stochastic function $s_2(\mathbf{r})$ to produce an output $v_2(\mathbf{r})$, the processing being repeated n times to produce function $v_n(\mathbf{r})$ where each stochastic function $s_n(\mathbf{r})$ is assumed to have been generated by the same (or different for a multiple-algorithmic protocol) key-dependent pseudo-random number generating algorithm subject to a different key.

D. Steganalysis

The method of encryption and information hiding considered is compounded in the following Fourier space-based equation:

$$H(\mathbf{k}) = F_2 + c\frac{S(\mathbf{k})}{\mid S(\mathbf{k}) \mid^2}\frac{F_2(\mathbf{k})}{\mid F_2(\mathbf{k}) \mid^2}F_1(\mathbf{k}) \tag{4}$$

where $H(\mathbf{k})$ coupled with equation (4) are known publicly (i.e., it is assumed that $h(\mathbf{r})$ can be intercepted and that the method of steganoencryption is known) and $F_2(\mathbf{k})$ is known privately; in effect, $F_2(\mathbf{k})$ is a private key known only to the sender and recipient of the function $H(\mathbf{k})$ together with the algorithm used for generating the key-dependent stochastic field $s(\mathbf{r})$.

From equation (4) it is clear that there is one known and three unknown functions (ignoring the value of c) and the problem of recovering $F_1(\mathbf{k})$ from $H(\mathbf{k})$ is ill-posed given that a well-posed problem has the following properties: (i) a solution exists; (ii) the solution is unique; (iii) the behaviour of the solution changes continuously with the initial conditions.

Consider the case where the covertext $f_2(\mathbf{r})$ and thus $F_2(\mathbf{k})$ is known. In this case, we can solve equation (4) and obtain a solution for $f_1(\mathbf{r})$ given by

$$f_1(\mathbf{r}) = s^*(\mathbf{r}) \odot w(\mathbf{r}) \tag{5}$$

where $w(\mathbf{r}) = c^{-1}\mathcal{F}_n^{-1}[H(\mathbf{k})F_2^*(\mathbf{k}) - \mid F_2(\mathbf{k}) \mid^2]$ and it is clear that can the plaintext $f_1(\mathbf{r})$ can now only be recovered, if and only if, the stochastic function $s(\mathbf{r})$ can be constructed. The problem is then reduced to the classic cryptanalysis problem, namely, given that the key-dependent algorithm for computing $s(\mathbf{r})$ is known, find the associated key(s). In this context, the application of a covertext function coupled with data diffusion prior to convolution based encryption provides a method for both hiding the cipher and enhancing the strength of the cipher given that the solution to equation (4) for $f_1(\mathbf{r})$ is ill-posed. Further, the diffusion of the function $f_1(\mathbf{r})$ with $f_2(\mathbf{r})$ prior to encryption (of the diffused field) provides a way of disguising any signature (statistical or otherwise) associated with cipher used.

Suppose that the plaintext function $f_1(\mathbf{r})$ happened to be known together with the covertext function $f_2(\mathbf{r})$ and the transmitted data $h(\mathbf{r})$; then from equation (5), it is clear that (using the correlation theorem) $s(\mathbf{r})$ can, in principle, be obtained from the equation

$$s(\mathbf{r}) = \mathcal{F}_n^{-1}\left[\frac{F_1^*(\mathbf{k})W^(\mathbf{k})}{\mid W(\mathbf{k}) \mid^2}\right],\ W(\mathbf{k}) = \mathcal{F}_n[w(\mathbf{r})]$$

But this result assumes that $\mid W(\mathbf{k}) \mid > 0 \forall \mathbf{k}$ illustrating that the de-correlation problem compounded in equation (5) is potentially ill-condition and therefore requires the application of the regularisation methods discussed in Section III, for example, for which only a non-unique estimate to the stochastic function $s(\mathbf{r})$ can be found.

Assuming that the de-correlation problem posed by equation (5) can be solved (in terms of generating a conditional estimate), this result illustrates the importance of changing the key and/or algorithm for computing $s(\mathbf{r})$. For a single algorithm protocol (in which the pseudo-random number generating algorithm is used repeatedly - the more usual case) and a key generating algorithm based on the covertext alone, the solution for $s(\mathbf{r})$ given above illustrates the importance of using a different covertext function for each stegotext transmission in order to minimise the potential for a successful attack. This requires a database of covertext functions to be created and shared prior to application of the method proposed. Such a database would ideally be communicated using a one-time-pad and a personalised encryption engine as discussed in [19], [21], [22] and [23], for example.

V. Case Study: Encrypted Image Hiding

Consider two digital images I_1 and I_2 of type real, each of which are regular matrices of size N×M whose elements are composed of floating point values between 0 and 1 inclusively (typically obtained by conversion to normalised floating point form from a k-bit image). Using the method discussed in Section IV, we now consider algorithms for encrypting/decrypting, hiding and recovering an image.

The plaintext image I_1 is encrypted using both data and stochastic diffusion and the output hidden in covertext image I_2 generating a stegotext image I_3 from which a decrypt I_4 is then generated, all processes being applied separately to each of the RGB components of colour input images. Clearly, the differences between I_2 and I_3 should be a minimum as should the difference between I_1 and I_4 which is examined later.

The method assumes the use of floating point arithmetic throughout including writing the stegotext image to file. For this reason, a Tagged Image File Format is considered in which the floating point data is retained. This is a fundamental requirement in order to recover the data prior to application of the inverse processes required to output a decrypt which is highly sensitive to (floating point) errors introduced into

the stegotext, thereby making the approach tamper-proof, i.e., floating point errors (subject to the floating point accuracy of the computations) introduced into the stegotext image through transmission noise or inspection by an attacker, including quantisation of the image, for example, leads to a erroneous decrypt.

Figure 1 shows an example of the application considered in this case study. Two test RGB colour images (with 8 bits per colour channel and of type .bmp) each of size 1024×768 are used to illustrate the method for a value of $c = 10^{-4}$ (the IEC). For this case (i.e., image size and type), the value of the IEC is optimal in terms of generating a stegotext with minimal distortion subject to a decrypt with minimal error (both in terms of the mean square error for each colour component), the visual differences between I_2 and I_3 and between I_1 and I_4 being insignificant. Diffusion of the images I_1 and I_2 is undertaken using a Fast Fourier Transform, as is the inverse process subject to the power spectrum being set to 1 if any spectral components are zero.

Fig. 1. Example of the encrypted image hiding application: Plaintext .bmp image (top-left) I_1, Covertext .bmp image (top-right) I_2, Stegotext .tiff image (bottom-left) I_3 and Decrypt .bmp image (bottom-right) I_4. Each image is a 1024×768 RGB colour image with 8 bits per colour channel.

The stochastic function $s(\mathbf{r})$ is computed using a conventional pseudo-random number generator which returns a uniformly distributed matrix of pseudo-random floating point numbers of size N×M with floating point values between 0 and 1 inclusively. However, it is well known that such conventional generators (i.e., linear congruential methods of pseudo-random number generation and 'Mersenne Twisters', for example) are cryptographically weak. Thus, in 'field operations' of the method discussed, the random number generating functions should be based on generators that are known to be cryptographically strong, and, ideally, personalised encryption engines using new classes of chaos-based algorithms obtained through the application of Evolutionary Computing and/or Artificial Intelligence, for example, [18] and [20].

The pseudo-random number generating functions used for stochastic diffusion (which implements the convolution encoding process) and the associated inverse process (which recovers the data) must or course use the same key which is set to the 'state' (the initial condition) of the random number generator. While these keys can, of course, be generated independently by the user, because the covertext image is critical to computing the decrypt, we consider using the covertext to generate the keys directly (given that the covertext is, in effect, a key). One way of doing this (and the way used in this Case Study) is by applying the equations (for each RGB colour component)

$$k_R = \lfloor \|aI_2^R\|_2 \rfloor,\ k_G = \lfloor \|aI_2^G\|_2 \rfloor \text{ and } k_B = \lfloor \|aI_2^B\|_2 \rfloor$$

where a is any large number whose magnitude determines the order of magnitude of the key length,

$$\|I\|_2 \equiv \sqrt{\sum_{n=1}^{N}\sum_{m}^{M} \mid I[n,m] \mid^2}$$

and $\lfloor x \rfloor \equiv \text{floor}(x)$ denotes an output that is the largest integer less than or equal to x.

It is envisaged that in the routine application of this algorithm, and, given that the keys used for stochastic diffusion are derived from the covertext, the sender and receiver of the stegotext would agree *a priori* upon a database of covertext images. Since the visual difference between the stegotext and covertext is insignificant, a visual inspection of the database using Thumbnails (i.e., reduced-size versions of the images contained in a database which serves the same role for images as a normal text index does for words as used by most modern operating systems or desktop and mobile environments) would be used to decrypt the encrypted image contained in the stegotext by the user choosing the image in the database that matches the received covertext. For large image databases, visual search engines could be used to produce a 'stegotext-covertext match'.

VI. Discussion and Conclusions

The use of personalised cryptographic algorithms coupled with the steganographic methods discussed in this paper and compounded in the application of Theorem 3.1, increases the threshold required for a successful attack to be launched in order to recover the plaintext. The attacker is first required to detect the existence of the encrypted information before an attempt can be made to decrypt it, the use of steganographic algorithms allowing for the existence of a ciphertext to be unknown. To recover the information, the attacker needs to first find a way of extracting the hidden encrypted information from the covertext and then decrypting it using the appropriate algorithm(s)/key(s). The exposure of the encryption key(s), the encryption algorithm(s) and the embedding technique to those other than the intended receiver is practically impossible provided, given the design of the key generating algorithm used in Section V, the covertext is not compromised, and a different covertext is used for each transmission. In this context, greater security would be provided if the key(s), and, ideally the pseudo-random number generating algorithm used for stochastic diffusion, were generated independently

from the covertext. This is of course at the cost of having to implement a separate key/algorithm-exchange protocol, under the fundamental cryptographic principle: *Ein messgeist, ein schlüssel, eine chiffre - One message, one key, one cipher*, a principle that underpins the use of a One-Time Pad (OTP), which yields ciphers that are unconditionally and computationally secure (i.e. secure given an upper bound on the computational capabilities of an adversary even in the context of a quantum computer given that an OTP is unconditionally secure, e.g., [24], [25]). In regard to the work reported here, this principle may be taken to be extended further to the following *Steganocryptographic law*: *One message, one key, one cipher, one covertext*.

The applications of the approach considered are numerous. Coupled with appropriate key-exchange protocols to initiate the use of cryptographically strong ciphers, the approach provides a generic method of encrypting and hiding high fidelity digital information, irrespective of the dimension of the data. The encrypted data is highly sensitive to transmission error and intolerant to distortion. The hidden data is therefore very fragile and hence, relatively tamper-proof. This is due primarily to the method of information hiding which relies on floating point addition so that truncation of the stegotext due to quantisation involving transformation from floating point to integer form is not possible as is lossy compression, for example. In regard to digital signal applications involving audio files, for example, this is not an issue because audio files are composed of streams of floating point data (ignoring application specific data formatting and compression). However, digital images commonly rely on 'depth-quantisation' so that they can be displayed and retained as arrays composed of integers. This is why Least Significant Bit methods are so popular in image-based steganography, a method which has not been applied in this case. Thus, a further investigation that would be of value is to research different data embedding techniques, [26], other than the floating point additive approach considered here which necessitates the output image file having to be written in floating point form. In this respect, MATLAB code and a prototype Python script for investigating the algorithms discussed in this paper, in particular, for the case study given in Section V, are available in [10].

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Dublin Institute of Technology, the University of KwaZulu-Natal and the Military Technological College, MoD, Oman.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, *Information Hiding: A Survey*, Proceedings of the IEEE (special issue), Vol. 87, No. 7, 1062-1078, 1999.

[2] The (UK) National Archives, *Regulation of Investigatory Powers Act 2000*, 2000. https://www.legislation.gov.uk/ukpga/2000/23/contents

[3] S. Katzenbeisser and F. A. Petitcolas, *Information Hiding: Techniques for Steganography and Digital Watermarking*, Artech House, Computer Security Series, 2000, ISBN: 1-58053-035-4.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography*, Morgan-Kaufmann, 2007. (e-Book) ISBN: 9780080555805.

[5] A. R. Al-Rawi, *Digital Rights Management using Steganocryptography*, PhD Thesis, Dublin Institute of Technology, 2013.

[6] J. M. Blackledge and E. D. Coyle, *Information Hiding by Stochastic Diffusion and its Application to Printed Document Authentication*, Proc. of IET ISSC2009, UCD June 10-11, 2009, Vol. 20, No. 1, PS-4, 1-6, 2009.

[7] J. M. Blackledge, *Information Hiding using Stochastic Diffusion for the Covert Transmission of Encrypted Images*, Proc of IET ISSC2010 UCC Cork, 23-24 June, 2010.

[8] J. M. Blackledge and A. R. Al-Rawi, *Steganography using Stochastic Diffusion for the Covert Communication of Digital Images*, IANEG International Journal of Applied Mathematics, Vol. 41, Issue 4, 270-298, 2011.

[9] J. M. Blackledge and A. R. Al-Rawi, *Image Authentication using Stochastic Diffusion*, Systems Informatics: Modelling and Simulation, UKSIM2013, 10-12 April, Cambridge University, 2013.

[10] J. M. Blackledge, P. Tobin, J. Myeza and C. M. Adolfo, *Information Hiding with Data Diffusion using Convolutional Encoding for Superencryption*, International Journal for Pure and Applied Mathematics (Mathematica Aeterna), Vol. 7, No. 4, 319-356, 2017. http://www.e-hilaris.com/MA/2017/MA7_4_2.pdf

[11] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press, 2003, ISBN-13: 9780521642989. http://www.inference.org.uk/mackay/itila/

[12] R. Khanai and G. H. Kulkarni, *Performance Analysis of Conventional Crypto-coding*, International Journal of Latest Trends in Computing 193 Vol. 2, Issue 1, 193-197, 2011, e-ISSN: 2045-5364.

[13] *Viterbi algorithm*, Wikipedia, the free Encyclopaedia. https://en.wikipedia.org/wiki/Viterbi_algorithm

[14] R. Morelos-Zaragoza, *The Art of Error Correcting Codes*, Wiley, ISBN: 0470015586. http://the-art-of-ecc.com/

[15] J. M. Blackledge, *Digital Signal Processing: Mathematical and Computational Methods, Software Development and Applications*, Edition 2, Woodhead Publishing: Series in Electronic and Optical Materials, 2006; eBook ISBN: 9780857099457. https://arrow.dit.ie/engschelebk/4/

[16] J. M. Blackledge, *Quantitative Coherent Imaging: Theory Methods and Applications*, Techniques in Physics, Academic Press, 1987; ISBN: 0-12-103300-7.

[17] J. M. Blackledge, *Digital Image Processing: Mathematical and Computational Methods*, Woodhead Publishing Series in Electronic and Optical Materials, 2005; ISBN-13: 978-1898563495. https://arrow.dit.ie/engschelebk/3/

[18] J. M. Blackledge, S. Bezobrazov, P. Tobin and F. Zamora, *Cryptography using Evolutionary Computing*, Proc. IET ISSC2013, Letterkenny, Co Donegal, Ireland, June 20-21, 2013.

[19] P. Tobin, J. M. Blackledge and S. Bezobrazov, *Personalised Encryptor Generation for the Cloud using Evolutionary Computing*, The International Workshop on Nonlinear Maps and their Applications (NOMA-2015), Dublin, Ireland, 15-16 June, 2015.

[20] J. M. Blackledge, P. Tobin and S. Bezobrazov, *Cryptography using Artificial Intelligence*, The International Joint Conference on Neural Networks (IJCNN2015), Killarney, Ireland, 12-17 July, 2015.

[21] P. Tobin, L. Tobin, J. M. Blackledge and M. McKeever, *Chaos-based Cryptography for Cloud Computing*, IET ISSC2016, Ulster University, Derry, Northern Ireland, June 21-22, 2016.

[22] P. Tobin, L. Tobin, J. M. Blackledge and M. McKeever, *On the Development of a One-Time Pad Generator for Personalising Cloud Security*, Eighth International Conference on Cloud Computing, Grids and Virtualisation, Athens, Greece February 19 - 23, 2017.

[23] P. Tobin, L. Tobin, J. M. Blackledge and M. McKeever, *A Hardware One-Time Pad Prototype Generator for Localising Cloud Security*, 16th European Conference on Cyber Warfare and Security (ECCWS 2017), University College Dublin, Dublin June 29-30, 480-487, 2017.

[24] Mils Electronic Gesmbh & Cokg*One Time Pad Encryption: The unbreakable Encryption Method*, http://www.cryptomuseum.com/manuf/mils/files/mils_otp_proof.pdf

[25] D. Rijmenantis, *The Complete Guide to Secure Communications with the One Time Pad Cipher* Cipher Machines & Cryptology, Ed. 7.4 - Jan. 22, 2016. http://users.telenet.be/d.rijmenants/papers/one_time_pad.pdf

[26] K. Saranya, C. S. Gnanadhas and M. George, *Data Embedding Techniques in Steganography*, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 3, Issue 2, 200-205, 2013.