Embedding Data in Images Securely using Chaos

Sai Venkatesh Balasubramanian

Sree Sai Vidhya Mandhir, Mallasandra, Bengaluru-560109, Karnataka, India.
saivenkateshbalasubramanian@gmail.com

Abstract

A robust high-fidelity technique to hide data in images using chaos is proposed and implemented. By efficiently harnessing the nonlinearity of a semiconductor device such as a MOSFET, a chaotic carrier signal is generated using extremely simple circuitry. This chaotic carrier forms the secure key of the proposed embedding system. The generated chaotic signal is validated using standard metrics such as Lyapunov Exponent, Fractal dimension and Kolmogorov Entropy. The generated carrier is then modulated with three message signals and are embedded into the three colors of the carrier image using a scaling factor. The exact frequencies and amplitudes used to generate the chaotic carrier are used in the receiver end to regenerate the carrier, using which the message is decoded from the embedded image. Standard measures such as Mean Square Error and Peak Signal to Noise Ratio are used to characterise the fidelity of the embedding process. The observed large PSNR values corresponding with high sensitivity as observed in the Lyapunov exponent of the chaotic carrier indicate the achievement of the golden advantages of Sensitivity, Fidelity and Simplicity which form the highlights of the present work.

Keywords: Information Security, Data Hiding, Secure Communication using Chaos, MOSFET, Encryption

1. Introduction

In the present era of information technology, the one phrase that keeps echoing in every nook and corner of the world is 'Big Data' [1]. As the data collection and processing capacity of the world as a whole is increasing at an exponential pace, there is a huge demand for attaining very high standards in terms of data throughput, processing capabilities and security, all at the same time [2, 3]. Most of these demands can be achieved by a shift of paradigm from the conventional linear signal approach to the more wholesome nonlinear signal approach [4, 5]. Such a nonlinear signal processing approach will greatly benefit handling and manipulating large amounts of data by effectively harnessing their phase relationships collectively [6, 7, 8], which is the hallmark of Big Data [1]. The most prominent beneficiaries in this era of Big Data are social networking sites and internet enabled services such as banking where privacy and security in data transmission is most crucial [1, 2, 3].

Among the various forms of secure data transmission using image as a platform, two techniques stand out. The first is steganography, with its key aim being imperceptibility to human senses [9]-[17]. Specifically, steganography pertains to the covert communication of a message in a multimedia based carrier such as an image [9]-[12]. To achieve this purpose, various techniques such as Chaffing and Winnowing, Mimic functions, fractionalized blog steganography and noise induced steganography are used [13]-[17].

The second is digital watermarking, a passive protection tool with robustness as the prime priority [18]-[22]. Digital watermarking is categorized by the various embedding techniques used such as additive spread spectrum, quantization and amplitude modulation [18]-[22].

While spread spectrum methods achieve modest amounts of robustness, they suffer from a low information capacity [9]. On the other hand, quantization based techniques offer high information capacity with limited robustness [17, 22].

The present work purports to an application oriented implementation of the nonlinear signal processing approach with image as the carrier and with a marked deviation from both of the above mentioned techniques. Specifically, the modulation and embedding techniques proposed in the present work relies on the delicate phase relationships of the modulated signal samples introduced due to nonlinearity and chaos [4]-[6]. This enables the amplitude variations to be minimal, enhancing the robustness of the system [9]-[22]. The advantage of high capacity in the present work can be conceptually elaborated as follows:

1. The spatial phase distribution of the modulated signal forms an ornamental pattern by itself as is evident from standard characterization such as phase portrait and bispectrum [4]-[6].
2. Embedding this onto the image is akin to embedding an innocent image (phase pattern) onto another innocent image (pixel pattern).

3. The minimal amplitude variations coupled with the flexibility of embedding offered in the phase domain enables high capacity in the present work. The extreme sensitivity provided by the chaotic signal used as carrier yields a very high level of security. These factors justify the twin advantages of security and capacity being obtained simultaneously, an improvement over both steganography and digital watermarking.

Based on the above mentioned concepts, the present work focuses on an application-oriented implementation of the nonlinear signal approach, thus demonstrating its efficiency in terms of error rate, system complexity and fidelity. Taking cue from the nonlinearity in the drain current - drain voltage characteristics of a semiconductor device such as MOSFET, an appropriate chaotic signal, that forms the crucial key for the embedding process, is generated [5] . The aforementioned chaotic carrier signal is then modulated by the message signal and embedded into the carrier image thereby enhancing the information security. The main aspects that encompass the enhancement of information security via the chaotic signal processing approach should be aimed towards achieving sensitivity, fidelity and simplicity. The aforementioned goals are quantitatively represented by metrics such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)[3, 23]. The present work purports to finding an appropriate solution for the accomplishment of the above mentioned goals.

2. Methodology

The proposed system is a hardware-dependent secure information embedding system using chaos using image as the embedding platform. The principles of nonlinearity and chaos are used to embed information in the phase of a hardware-generated carrier signal. The block diagram illustrating the embedding procedure is as shown in Fig.(1).

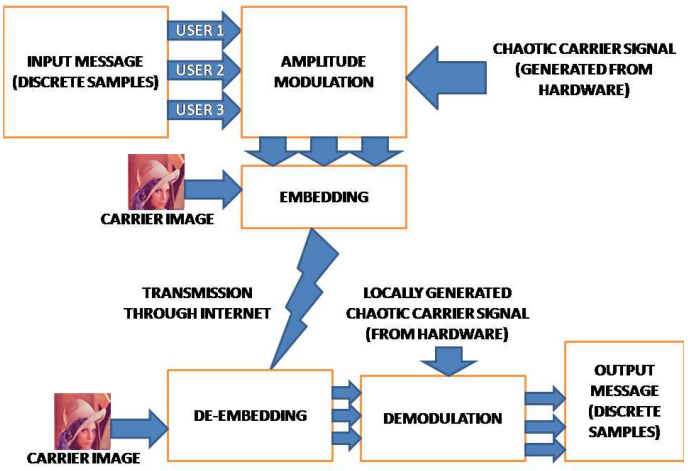

Figure 1: Block Diagram of the Proposed Steganographic Embedding System

2.1. Generation of Chaotic Carrier Signal

The first step in the proposed system is the generation of chaotic carrier signal. In order to achieve this, the nonlinearity of a semiconductor device such as a N-MOSFET is used [5].

The nonlinearity of the NMOSFET can be understood from the nonlinear dependence of the drain current I_d on the drain voltage V_D and the gate voltage V_G, as seen from Equation 1, valid for the nonlinear point between the linear and saturation regions [24].

$$I_d = \frac{\mu_n Z C_i}{L}\left[\left(V_G - V_{FB} - 2\psi_f - \frac{V_D}{2}\right)V_D - \frac{2}{3}\frac{\sqrt{2\epsilon j_s q N_a}}{C_i}\left[(V_D + 2\psi_f)^{1.5} - (2\psi_f)^{1.5}\right]\right] \quad (1)$$

Here μ_n denotes the electron mobility, C_i the intrinsic capacitance, V_{FB} is the flat band voltage, j_s is the current density, q is the charge, N_a is the acceptor concentration, ψ_f denotes the work function and L and Z denote the transistor geometry parameters.

It is noted that the nonlinear, specifically fractional dependence of the output of a single transistor on the input signals (the 1.5 exponent in Equation 1) is responsible for the generation of chaotic signals, to be used as carriers of

information in the present work. Two sinusoidal signals are given as inputs to the gate and the drain of the MOSFET. The output is taken from the source terminal. By adjusting the amplitudes of the sinusoidal signals such that they lie in the knee region of the MOS transfer characteristics, nonlinearity is achieved [5]. In the present work, the N-Channel power MOSFET MTP50N06E is used and the schematic and experimental setup to generate chaos are shown in Fig. (2) and Fig. (3) respectively. The amplitude of the drain and the gate signals are chosen as 5Vrms and 2Vrms respectively. By suitably selecting the frequencies of the gate and drain signals, proper disharmony between the signals is achieved leading to chaos. By selecting the gate frequency as 4MHz and the drain frequency as multiples of the gate frequency such as 8MHz, 12MHz and so on, period doubling, tripling etc can be achieved, with non integer ratios such as 3:12.1 giving chaos. The experimental results for two such cases, the period tripling with a frequency ratio 4:12 and a chaotic case with 4:12.1 are illustrated in Fig. (4).

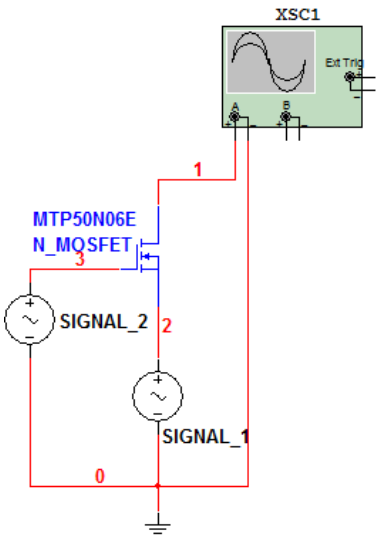

Figure 2: Schematic of Chaotic Carrier Generation

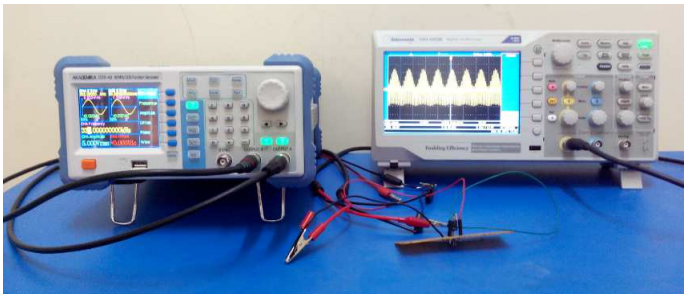

Figure 3: Experimental setup of Chaotic Carrier Generation using Power MOSFET MTP50N06E.

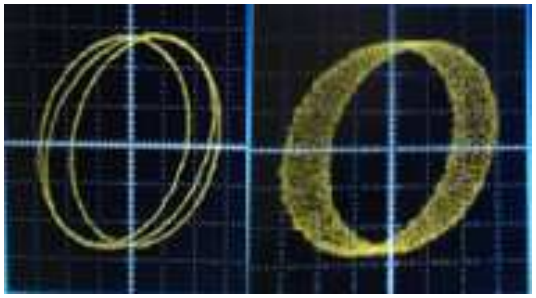

Figure 4: Experimental Results of period tripling and chaotic cases

The above results confirm the hypothesized chaotic behavior arising out of a single transistor. In the present work, the base frequency for the gate input is selected as 35kHz. Firstly, the drain signal frequency is set to 70kHz so that it is twice that of the gate signal frequency. In this case, the nonlinearity of the MOSFET gives rise to periodic doubling, as seen in the waveform and phase portraits in Fig.(5) and Fig.(6). This signifies the onset of instability in the MOSFET, leading in due course to chaos [6, 7].

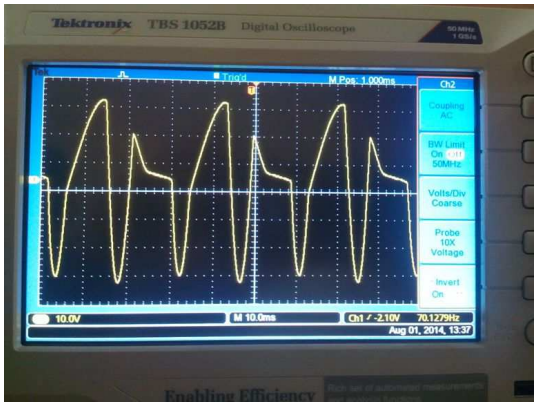

Figure 5: Output Voltage Waveform of the period 2 signal.

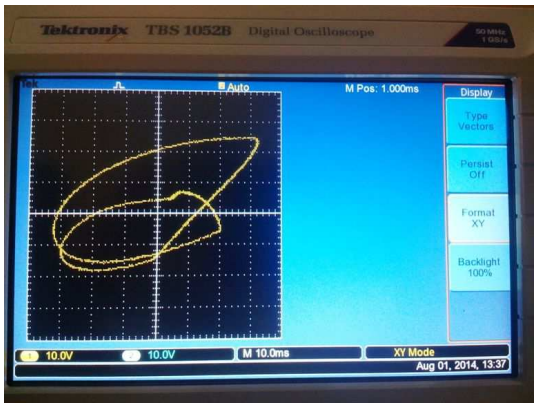

Figure 6: Phase portrait of the period 2 signal.

When the drain frequency is set to a non integer multiple of the gate frequency such as 332kHz, chaos is observed. In order to better understand the properties of the generated chaotic signal, the phase portrait, waveform and spectrum are plotted and are shown in Figs.(7),(8) and (9)). The fractal dimension of this signal is calculated using the Minkowski Bouligand box counting algorithm and is obtained as in Fig.(12). The fractal dimension of around 0.7 clearly indicates the presence of chaos, arising in particular to the fractional (non-integral) frequency ratios of the gate and drain signal. Also, the largest Lyapunov Exponent computed using the Rosenstein algorithm is obtained as 9.2385 [28, 29]. The corresponding divergences of nearest trajectories are illustrated in Fig.(13).The high value of Lyapunov exponent highlights the sensitivity of the carrier signal to the frequencies of the drain and gate signals [27, 28, 29].

The characterization of the frequency dependant chaos can be studied using an iterative equation where the frequency ratio r = f2/f1 acts as the control parameter [4]-[6]. The iterative equation is given as follows where $f_o(i)$ represents the ith component of the output frequency.

$$f_o(i+1) = mod(f_o(i) + \frac{f_2}{f_1} - V(f_o(i)), \pi) \tag{2}$$

Here the f_o terms denote the output frequencies, whereas f_1 and f_2 denote the frequencies of the input signals. $V(f_o)$ denotes the input signal waveform employed in the chaotic system. The bifurcation diagram corresponding to the above equation is given in Fig. (10.)

As can be seen, the bifurcation diagram shows a periodic trend, with order being seen at f2/f1 being integer or half-integer multiples, and chaotic otherwise. Thus, if the frequency ratios are chosen in the chaotic regime, like the ones

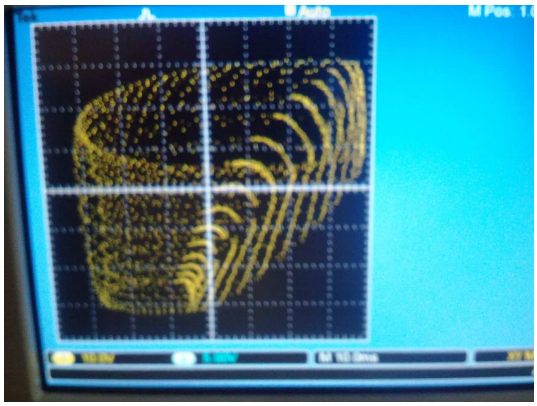

Figure 7: Experimentally obtained Phase portrait of the Chaotic carrier generated.

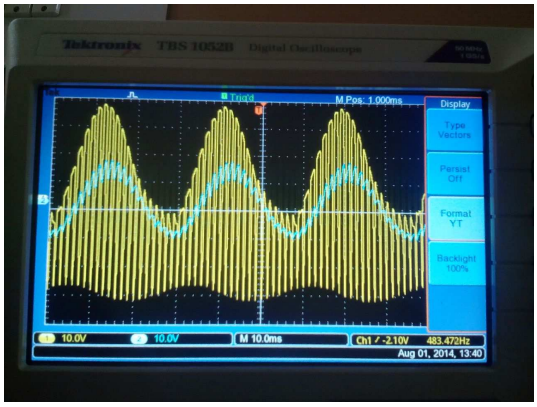

Figure 8: Voltage Waveform of the Chaotic carrier generated.

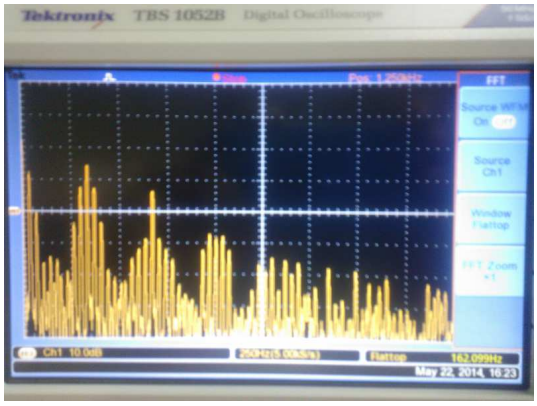

Figure 9: Magnitude Spectrum of the Chaotic carrier generated.

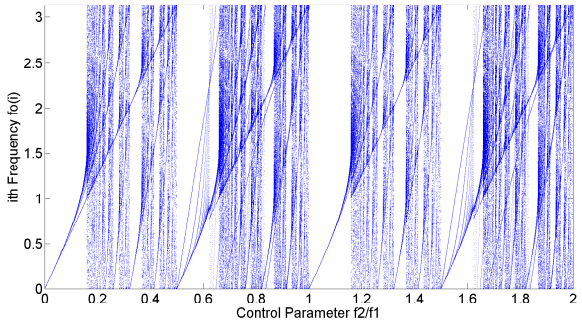

Figure 10: The Bifurcation Plot

chosen in the present work (332/35 corresponding to mod value of 0.485), then said ratio forms an extremely secure key, since, in order to demodulate in the receiver end, the exact same frequency alone can results in successful decoding. Even a slight deviation from the ratio results in erroneous results. To understand the significance of the transistor nonlinearity in generating chaos, the bispectrum is plotted. The bispectrum is the spectrum obtained from the third order cumulant, and for any two given frequencies f1 and f2, the bispectrum of a signal displays the frequency components f1 and f2 and the cross coupling components f1+f2 [30]. The bispectrum of the generated chaotic signal is shown as follows:

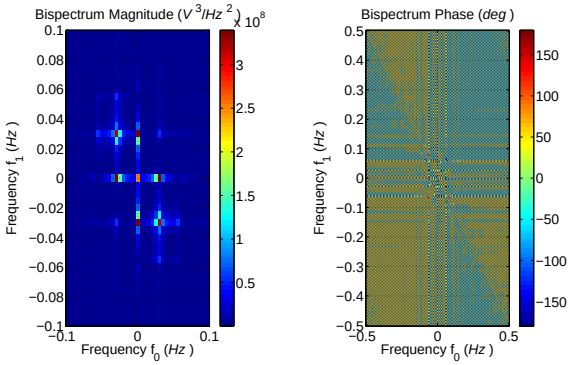

Figure 11: Bispectrum before modulation

As can be seen from the bispectrum, the magnitude spectrum shows cross modulation products in the normalized frequency range of -0.05 to 0.05. Significant distribution in phase spectrum is seen. The cross modulation products arise entirely due to transistor nonlinearity as explained earlier. The information capacity of the generated chaotic carrier signal is characterized by the Kolmogorov Entropy [1, 31, 32, 33], which is obtained as 4.709 nats/symbol or equivalently, 6.79 bits/symbol. This relatively high value of the Kolmogorov entropy indicates that the chaotic carrier signal serves to carry a reasonably large amount of information, thus testifying to the concept of Big Data [1, 31, 32, 33].

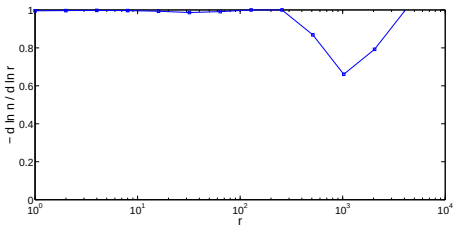

Figure 12: Fractal Dimension of the Chaotic carrier generated. Here, r denotes the size of boxes used in the box counting algorithm, and n denotes the corresponding number of boxes.

2.2. Modulation

The next step is to modulate the generated chaotic carrier using the message signal. The modulation used here is Amplitude modulation. In order to completely utilize the data embedding capabilities, 3 different messages from three

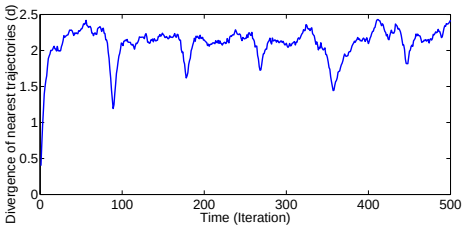

Figure 13: Rosenstein Algorithm results for the chaotic carrier signal.

distinct users are generated, corresponding to the red, green and blue pixel distributions in an image. Each message is represented in the present work by a discrete sampled array of a sinusoidal wave. In the present work, the three message signal frequencies are 35kHz, 70kHz and 105kHz such that they form a ratio 1:2:3. The message signals of the three users are illustrated in Fig. (14), Fig. (15) and Fig. (16).

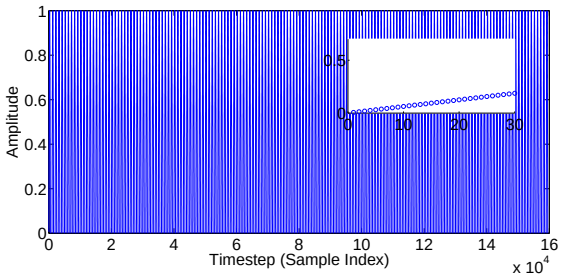

Figure 14: Message Signal of User 1. Inset: First 10000 samples.

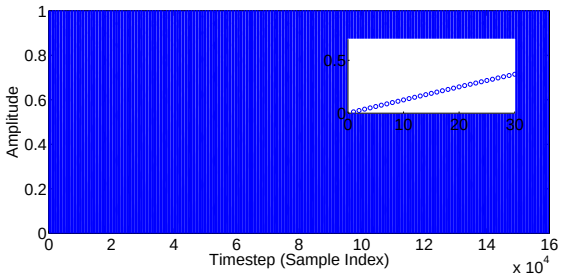

Figure 15: Message Signal of User 2. Inset: First 10000 samples.

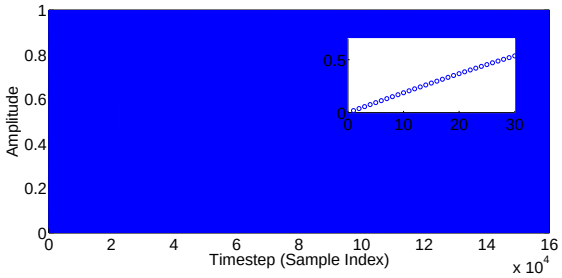

Figure 16: Message Signal of User 3. Inset: First 10000 samples.

The messages of the three users are modulated using the chaotic carrier signal shown in Fig. (8). As an illustration, the modulated signal for User 1 is shown in Fig. (17).

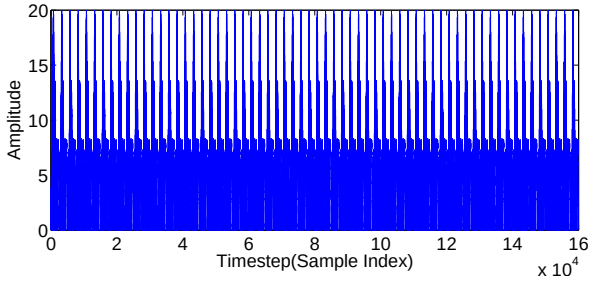

Figure 17: Message Signal of User 1 Modulated using Chaotic Carrier.

The phase portraits of the three modulated signals are plotted in Figs. (19), (20) and (21).The modulation is characterized by comparing the bispectra of the chaotic carrier before and after modulation. The bispectrum of the modulated signal is as follows.

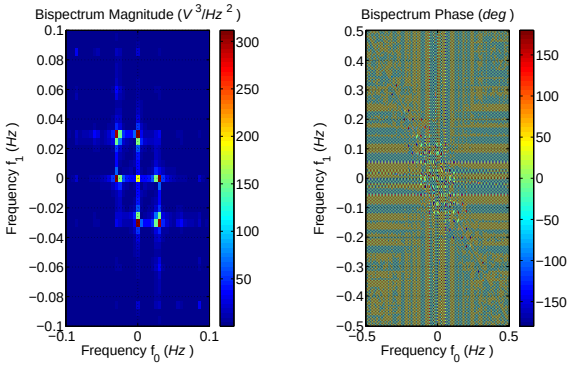

Figure 18: Bispectrum after modulation.

As can be seen, while both the magnitude bispectra look almost similar, distinguishing patterns are found in the phase bispectra. This confirms the bottomline of the present work: embedding information in phase. It is this phase embedding that yields the high information capacity and security reported in this work.

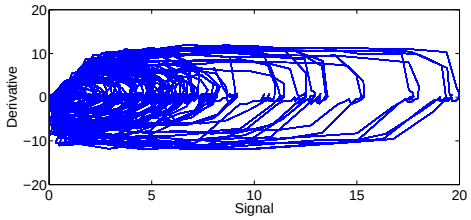

Figure 19: Phase Portrait of Modulated Signal of User 1

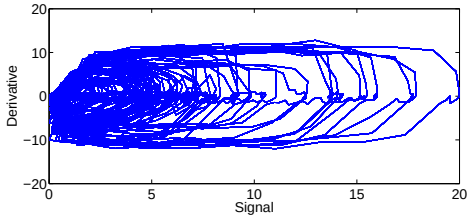

Figure 20: Phase Portrait of Modulated Signal of User 2

2.3. Embedding the modulated signal in the Carrier Image

In the present work the carrier image is chosen as Lena of 400x400 resolution(.png format). An embedding rate of

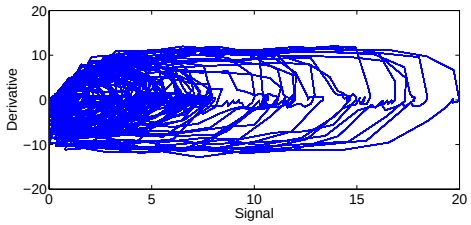

Figure 21: Phase Portrait of Modulated Signal of User 3

one sample per pixel is used, which implies that each of the three color arrays (red, green and blue) can hold 160000 samples. Considering conventional ASCII coding, each sample corresponds to 8 bits. Thus each pixel of the 400x400 color image holds 24 bits of message information.

In order to increase the robustness of the proposed steganographic process, the amplitudes of the three modulated signals are scaled down to a small fraction (around 1-5 percent) of the maximum pixel intensity (255). For each of the three arrays of Red, Green and Blue, each sample of the corresponding modulated signal is scaled down to a factor of around 1 percent of the maximum pixel value intensity 255, thus resulting in a scaling factor of 2. These scaled down samples are added to the image pixel values. After repeating this process for the other two colours, the components of the image are rejoined to give the embedded image. The original carrier image and the embedded image are shown in Figs. (22) and (23).

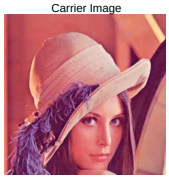

Figure 22: Carrier Image Lena before embedding

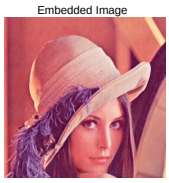

Figure 23: Carrier Image Lena after Embedding

Though the above mentioned embedding looks eerily similar to additive spread spectrum steganography, the fact that the addition of message amplitude to the chaotic carrier reflects in its phase, rather than its amplitude, as witnessed in the bispectrum, amply highlights the uniqueness of the embedding process. Also, by setting the scaling factor to a low value (1 percent), extreme robustness is achieved.

The chaotic properties of the embedded image are studied. Firstly, the spatial FFT of the image is plotted in Fig. (24). The underlying patterns in the FFT testify to the fact that the information is embedded into the phase of the image [34].

In order to better understand the changes in the carrier image induced due to the embedding process, the red, green and blue histogram of the carrier and embedded images are plotted in Fig. (25) - Fig. (30).

The embedded image is now transmitted through the internet or equivalent transmission channel.

2.4. Receiving the Message

At the receiver end, the chaotic carrier is generated individually by using the circuit given in Fig. (2). To detect the hidden message, the image is first split up into Red,Green and Blue components, and the carrier image components is subtracted from the corresponding received image components to reveal the three modulated signals. Then, using the locally generated chaotic carrier, amplitude demodulation is performed, and the outputs are the three required message signals. The received message signals for the three users are plotted in Fig. (31), Fig. (32) and Fig. (33).

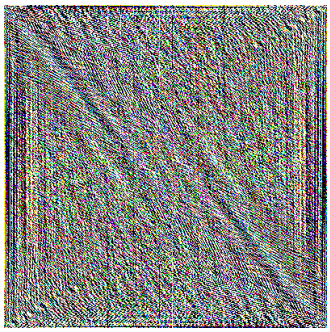

Figure 24: Spatial FFT of the image

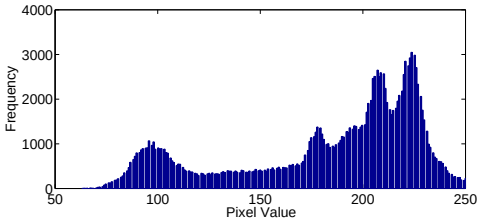

Figure 25: Red Pixel Histogram before Embedding

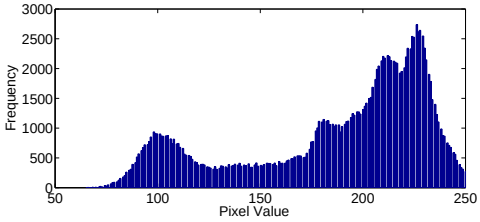

Figure 26: Red Pixel Histogram after Embedding

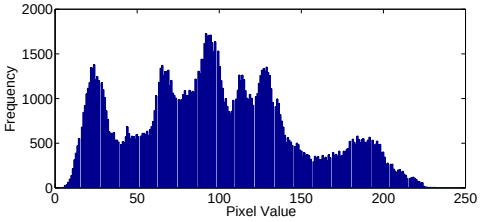

Figure 27: Green Pixel Histogram before Embedding

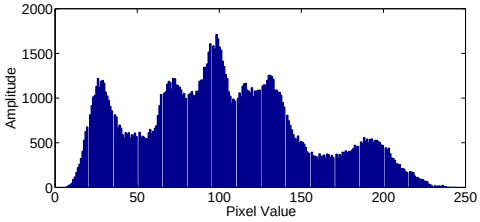

Figure 28: Green Pixel Histogram after Embedding

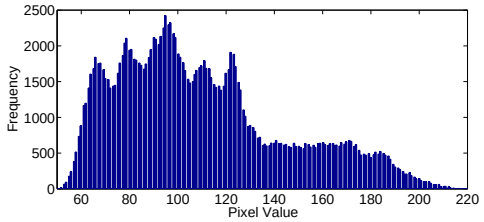

Figure 29: Blue Pixel Histogram before Embedding

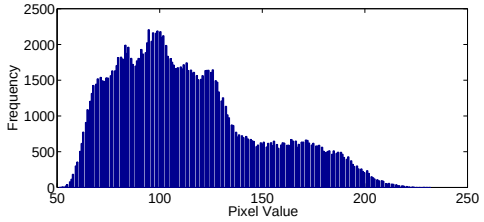

Figure 30: Blue Pixel Histogram after Embedding

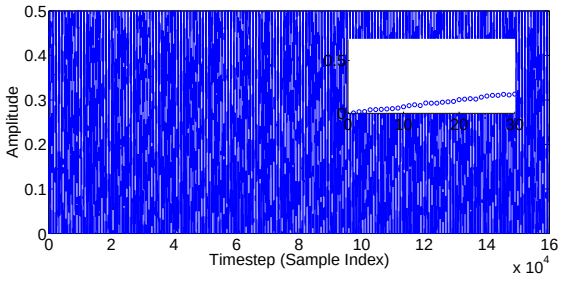

Figure 31: Received Signal for User 1. Inset: First 30 samples.

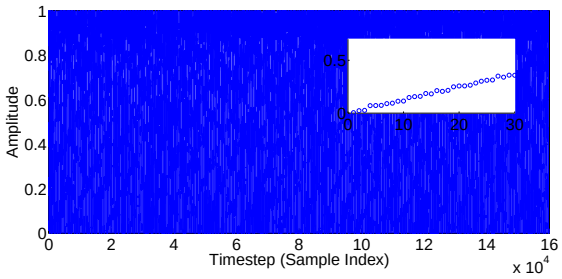

Figure 32: Received Signal for User 2. Inset: First 30 samples.

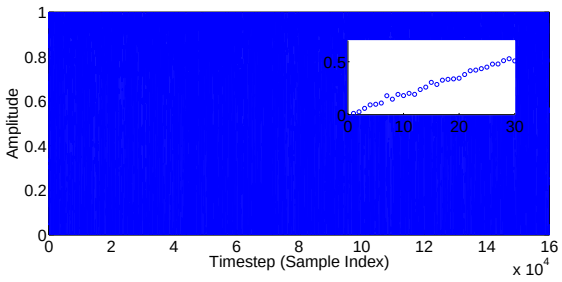

Figure 33: Received Signal for User 3. Inset: First 30 samples.

3. Performance Assessment

3.1. Sensitivity

The success of detecting the message heavily depends on the accuracy of the locally generated chaotic carrier. Even a slight mismatch of the local chaotic carrier to its transmitting counterpart yields a drastically different detected signal, owing to the extreme sensitivity of chaos to initial conditions. Thus, a proper decoding of the message only occurs when the drain and gate signal voltages and frequencies match exactly to the ones used during transmission. In order to highlight this point, a sample of two different chaotic signals generated, one with a frequency ration of 35:332 and other with a ratio of 36:332 are illustrated in Fig. (34). It is clearly seen that after the first few cycles, the two signals vary significantly. This ensures that the message demodulated using any ratio different from the transmitted one will certainly be erroneous.

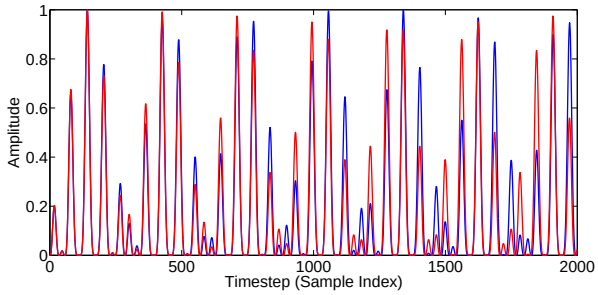

Figure 34: Samples of two chaotic signals generated using different frequency ration - 332:35 (blue) and 332:36 (red).

The drain to source frequency ratio thus forms a very secure 'key' of the embedding process. Since the key is an analog value of frequency, it is not limited by bit capacity unlike the 128-bit or similar encryption 'passwords' used by typical digital systems [9]-[22]. Thus the embedding process can accomodate an extremely large number of users without significant repetition of key. This ensures a very high level of security in the message transmission process, which is a characteristic highlight of the present work.

3.2. Fidelity

In order to characterize the fidelity of the embedding process, the peak signal to noise ratio (PSNR) is computed by comparing the raw carrier image and the embedded image [23]. It is observed that the PSNR varies with respect to the scaling factor used to embed the modulated signal into the image. This variation of PSNR with scaling factor is plotted for all the three color components in Fig. (35). The PSNR at the default scaling factor of 2 is obtained at around 50-52dB. The corresponding Mean Square Error value is obtained around 0.45.

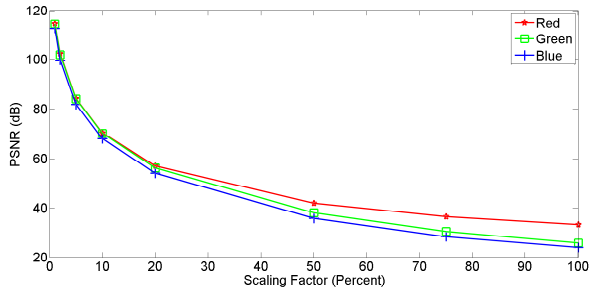

Figure 35: PSNR as a function of scaling factor for Carrier Image Lena (PSNR Calculated using natural logarithm)

The high sensitivity of the embedding process can be characterized by plotting the Lyapunov exponents for the three colors in the embedded image. This is shown in Fig. (36) to Fig. (38). The corresponding largest Lyapunov exponents for red, green and blue are obtained as 16.2833, 16.2833 and 12.3778. The positive Lyapunov exponents obtained for the three color components ascertain the presence of chaos in the embedded images. Thus, high sensitivity is achieved [27, 28, 29].

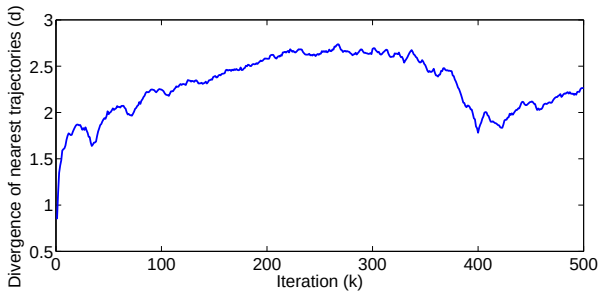

Figure 36: Rosenstein algorithm result for red pixel distribution in the embedded image.

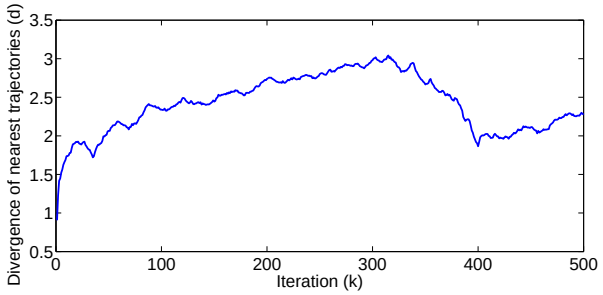

Figure 37: Rosenstein algorithm result for green pixel distribution in the embedded image.

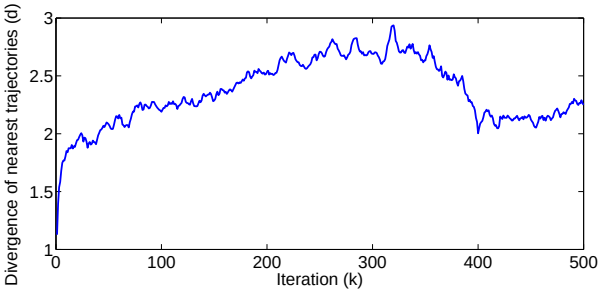

Figure 38: Rosenstein algorithm result for blue pixel distribution in the embedded image.

Table 1: Tabulation highlighting K2, LLE, PSNR and MSE for various message frequencies

Test Case	Color	Freq (KHz)	K2 (nats/s)	LLE	MSE	PSNR (dB)
1	Red	35	4.928	16.2833	0.4701	51.4
	Green	70	5.215	16.2833	0.4180	51.89
	Blue	105	4.833	12.3778	0.4412	51.69
2	Red	332	4.928	15.6832	0.4091	52.01
	Green	664	5.215	15.6832	0.4380	51.69
	Blue	996	4.833	12.2688	0.4180	51.89
3	Red	332	4.928	15.6832	0.4091	52.01
	Green	332	5.215	15.6832	0.4108	52
	Blue	332	4.833	13.5109	0.4108	52
4	Red	1700	4.928	16.8757	0.4140	51.96
	Green	1700	5.215	16.8757	0.4160	51.94
	Blue	1700	4.833	13.1732	0.4160	51.94
5	Red	17	4.928	17.1953	0.6318	50.12
	Green	17	5.215	17.1953	0.6348	50.10
	Blue	17	4.833	14.9102	0.6348	50.10

Table 2: PSNR Comparison with Steganographic and Watermarking Techniques

Technique	Category	Reported PSNR Value (dB)
Spread Spectrum Steganography [9]	Steganography	30
Image Downsampling [14]	Steganography	51.14
Uniform Embedding [15]	Steganography	51.5
Dither Modulation [18]	Watermarking	40
Lossless Data Embedding [20]	Watermarking	35
Quantization Index Modulation [21]	Watermarking	30

3.3. Simplicity

The simplicity of the proposed embedding process is characterised by two main factors. The first is the extremely simple circuit used to generate the chaotic carrier signal, and this is owing to the effective harnessing of the MOS nonlinearity. The second factor is that in spite of using simple techniques like raster based embedding in the image, a high value of PSNR is obtained.

3.4. Effect of Scaling Factor and Frequency on Performance

In order to understand the suitability of the proposed embedding process to input frequency, the standard parameters of PSNR, MSE, K2 and Lyapunov Exponents for various input frequencies are tabulated in table 1.

The table shows five different cases of frequencies for the Red, Green and Blue users in relation to the two frequencies used to generate the chaotic carrier (35kHz and 332kHz). In the first case, the R,G and B user frequencies are set in the ratio 1:2:3 with the R frequency equal to the lower carrier frequency (35kHz). The second case also corresponds to 1:2:3 ratio but with the R frequency corresponding to the higher carrier frequency (332kHz). The third case is a case of resonance with all three frequencies set to the higher carrier frequency (332kHz). The fourth case illustrates a case of very high frequency for all three users (1.7MHz) whereas the fifth case illustrates a very low frequency for all three users (17kHz). Of all these cases, the third case, corresponding to a complete resonance at 332kHz results in the highest value of PSNR and the lowest value of MSE, corresponding to maximum fidelity.

In order to ascertain the performance of the techniques proposed in the present work with state-of-the-art steganographic and watermarking based techniques, the typical PSNR values reported in the literature for selected steganographic and watermarking techniques are tabulated in Table 2 [9]-[22]. It is noteworthy that even though the proposed technique embeds the data as discrete samples rather than digital bits, to ensure a fair comparison, the PSNR is reported in dB which is obtained by using a base-10 logarithm instead of the natural logarithm.

4. Conclusion

By effectively using the nonlinearity of a MOSFET, a chaotic signal is generated, and is used as a carrier for embedding a message securely in an image. The proposed system is implemented in hardware, and the performance is assessed by using metrics such as MSE and PSNR. The observed low values of MSE and high PSNR, leading to high fidelity and secure robust hiding mechanism, combined with extreme simplicity of the system forms the novelty of the present work. The usage of an analog frequency ratio value as the secure key ensures that a large number of users can be accommodated without repetition of key and thus the present work testifies to the concept of 'transformation through information'.

References

[1] X.Wu, X.Zhu, G.Q.Wu and W.Ding, *Data mining with big data*, IEEE Trans. on Knowledge and Data Engineering **26**,97-107(2014).
[2] P. Zhou, B.Zhao, J.Yang, Y.Zhang, *Throughput enhancement for phase change memories*, IEEE Trans. on Computers **63**,2080-2993(2014).
[3] J. Jacobs and B. Rudis, *Data-Driven Security: Analysis, Visualization and Dashboards* ,(Wiley, Indiana, 2014).
[4] K. E. Barner and G. R. Arce, *Nonlinear Signal and Image Processing: Theory, Methods, and Applications* ,(CRC Press, U.S, 2003).
[5] M. E. Inchiosa, A. R. Bulsara, A. D. Hibbs, and B. R. Whitecotton, *Signal Enhancement in a Nonlinear Transfer Characteristic*, Phys. Rev. Lett.**80**,1381(1998).
[6] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering* ,(Westview Press, Cambridge, 2008).
[7] E.Bilotta and P.Pantano, *A gallery of Chua attractors*,(World Scientific, Singapore, 2008).
[8] M. Cross and H. Greenside, *Pattern Formation and Dynamics in Nonequilibrium Systems* ,(Cambridge University Press, Cambridge, 2009).
[9] L. M. Marvel, C. G. Boncelet and C. T. Retter, *Spread Spectrum Image Steganography*, IEEE Trans. on Image Processing **8**,1075-1083(1999).
[10] N. F. Johnson, and S. Jajodia, *Exploring Steganography: Seeing the Unseen*, Computer **31.2**,26-34(1998).
[11] N.Hopper, L.VonAhn and J.Langford, *Provably secure steganography*, IEEE Trans. on Computers **58**,662-676(2009).
[12] F. Huang , J. Huang and Y. Q. Shi, *New Channel Selection Rule for JPEG Steganography*, IEEE Trans. on Information Forensics and Security **7**,1181-1191(2012).
[13] B. Li, S. Tan,M. Wang and J. Huang, *Investigation on Cost Assignment in Spatial Image Steganography*, IEEE Trans. on Information Forensics and Security **9**,1264-1277(2014).
[14] J. Kodovsky and J. Fridrich, *Effect of Image Downsampling on Steganographic Security*, IEEE Trans. on Information Forensics and Security **9**,752-762(2014).
[15] L. Guo , J. Ni and Yun Qing Shi, *Uniform Embedding for Efficient JPEG Steganography*, IEEE Trans. on Information Forensics and Security **9**,814-825(2014).
[16] Y. C. Tseng and H.K.Pan, *Data Hiding in 2 color images*, IEEE Trans. on Computers **51**,873-878(2002).
[17] J.M.Guo and T. N. Le, *Secret Communication Using JPEG Double Compression*, IEEE Signal Processing Letters **17**,879-882(2010).
[18] B. Chen and G. Wornell, *Digital Watermarking and Information Embedding using Dither Modulation*, IEEE Multimedia Signal Processing, **98**,273-278(1998).
[19] P. Bateman and H. G. Schaathun, *Image Steganography and Steganalysis*, (University of Surrey, UK, 2008).
[20] J. Fridrich and M. Goljan and D. Ru, *Lossless Data EmbeddingNew Paradigm in Digital Watermarking*, EURASIP Applied Signal Processing, **2**,185-196(2002).
[21] B. Chen and G. Wornell, *Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding*, IEEE Trans. Information Theory, **47**,1423-1443(2001).
[22] I. J. Cox, M. L. Miller, J. A. Bloom, *Digital Watermarking*, (Morgan Kaufmann, US, 2001).
[23] H. J. Zepernick and A. Finger, *Pseudo Random Signal Processing: Theory and Application* ,(Wiley, Indiana, 2013).
[24] B. G. Streetman and S. K.Banerjee, *Solid State Electronic Devices*,(PHI, U.S, 2006).
[25] D. Huang and S. Meyn, *Generalized Error Exponents for Small Sample Universal Hypothesis Testing*, IEEE Trans. on Information Theory **59**,8157-8189(2013).
[26] D.Teguig, V.Le Nir and B.Scheers, *Spectrum sensing method based on goodness of fit test using chi-square distribution*, IEEE Electronics Letters **50**,713-715(2014).
[27] S. P. Dawson, *Strange Nonattracting Chaotic Sets, Crises, and Fluctuating Lyapunov Exponents*, Phys.Rev. Lett **76**, 4348-4351(1996).
[28] J. P. Eckmann, S. O. Kamphorst, D. Ruelle and S. Ciliberto, *Liapunov exponents from time series*, Phys.Rev. A **34**, 4971-4979(1986).
[29] M. T. Rosenstein, J. J. Collins and C. J. De Luca, *A practical method for calculating largest Lyapunov exponents from small data sets*, Physica D, **65**,117-134(1993).
[30] M. A. Wolinsky, *Invitation to the Bispectrum*,(Defense Technical Information Center, USA, 1988).
[31] P. Grassberger and I. Procaccia, *Estimation of the Kolmogorov entropy from a chaotic signal*, Phys. Rev. A **28**,2591-2593(1983).
[32] Y. Termonia, *Kolmogorov entropy from a time series*, Phys. Rev. A **29**,1612-1614(1984).
[33] D. Salomon, D. Bryant and Giovanni Motta, *Handbook of Data Compression*,(Springer, California, 2010).
[34] S. Marshall and G. L. Sicuranza, *Advances in Nonlinear Signal and Image Processing*,(Hindawi, New York, 2006).