Optical Field Encryption for secure transmission of data

Colin Fraser, Andrew R Harvey
School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, EH14 4AS, Scotland, United Kingdom

Patent Application: GB0405573.7

ABSTRACT

The growing awareness of the vulnerability of information transmitted on communication systems within the government, military and commercial sectors, has stimulated a number of areas of research within the optical community to design optical hardware encryption systems providing inherent immunity to espionage techniques. This paper describes a hardware optical encryption technique that utilises off the shelf telecommunication equipment and negates the necessity for an independent key distribution system with respect to the data transmission system, as is common with alternative encryption system implementations. This method also lends itself easily to fiber optic or free space communication and is applicable within any optical waveband. The encryption-decryption of the optical signal is achieved through low coherence optical interferometry. This requires the instantaneous processing and analysis of the signal, optically, to retrieve the relevant optical phase information hidden in the transmitted optical noise. This technology allows an authorised user to transmit encrypted information at a high data rate securely, while maintaining opaqueness to an unauthorised observer that data transmission is occurring. As the instantaneous optical field properties of the signals present in the system are essential to the optical encryption - decryption process, the system is inherently protected against electronic recording and advances in computational decryption algorithms. For organisations wishing to protect sensitive data and levels of communication activity these are highly desirable features.

Keywords: Optical encryption, hardware security systems, multi-wavelength communication, free space communication

1. INTRODUCTION

Current network security, both intra- and inter-network, relies on software encryption to prevent transmitted data from being read by an unauthorised observer. Where additional security is required, for instance by Government Agencies and Financial institutions, dedicated communication links are deployed. Although this strategy consists of a closed encryption unit (the encryption and decryption units are assumed to be held in a secure establishment; the transmission system is in the public domain.) and a closed decryption unit, the transmission system between the units is still open, and therefore still relies primarily on software encryption of the data being transferred to counter any espionage activities. The assumption behind software encryption algorithms is that they cannot be compromised, based on current known mathematical principles and algorithms, in an acceptable time frame before the encoded data becomes obsolete. To counter any perceived advances in mathematical decryption algorithms and technology advances, ever-longer software encryption codes are employed. Unfortunately, if an algorithm becomes compromised the organisation employing the relevant coding algorithm is invariably the last to discover. A second, more subtle, disadvantage of employing software encryption on current optical intensity modulated telecommunication networks is that of activity level. If a Vernam (Gilbert Vernam 1917) one-time pad code is being applied to data, in theory, an unwanted observer cannot decipher the data without the unique decryption key. However, the unwanted observer can monitor network traffic volumes and their destination and be alerted to potential activities.

Due to concern over the security of software encryption, research into encrypting the data within the optical properties of the carrier wave itself is being investigated worldwide [1,2,3,4]. A prevalent optical phenomenon that provides an inherent means of burying data within a noisy background, while transmitting information from the source, is that of White Light Interferometry. This phenomenon is ubiquitous in nature and finds a partial application in the fields of

Advanced Free-Space Optical Communications Techniques and Technologies,
edited by Monte Ross, Andrew M. Scott, Proceedings of SPIE Vol. 5614
(SPIE, Bellingham, WA, 2004) · 0277-786X/04/$15 · doi: 10.1117/12.580310

remote Fiber Optic Sensors [5] and Surface Tomography [6,7]. In the Optical Field Encryption technique proposed here, the information to be communicated is embedded in the random phase fluctuations of the spectral content comprising a broadband optical source's output. By applying the principles of white light interferometry, this composite optical signal is then optically encrypted. To subsequently decrypt the original information from the optical source's spectral content, a hardware decryption configuration having unique physical parameters defined by it's corresponding encryption unit must be realised. By employing the methods used in Optical Fourier Transform spectroscopy the Optical Field Encryption technique can be realised either in optical fiber or free space forms.

2. PRINCIPLES OF OPERATION

In the optical field encryption technique proposed here, a tandem interferometer arrangement performs the signal encryption and decryption operations, optically. One interferometer performs the role of the encryption unit and the other that of the decryption unit. The optical encryption unit phase modulates the data to be transmitted onto the spectral content of an optical broadband source and then encrypts the resulting signal. This can be accomplished by splitting the output of the optical broadband source into two signals, $E_1(t)$ and $E_2(t)$, through amplitude division. One of the signals, $E_2(t)$ for instance, forms an optical reference signal containing the optical sources' spectral phase, polarisation and amplitude content at time t. This signal is transmitted directly to the decryption unit over the communication link. The second optical signal, $E_1(t)$, whose complex optical field spectrum is a replica of $E_2(t)$, is phase modulated by the data to be transmitted,

$$E_1(t) \rightarrow E_1(t+\theta(t)).$$

A predetermined temporal optical delay, τ_1, or equivalent optical phase shift, on the longitudinal path of E_1 is then applied,

$$E_1(t+\theta(t)) \rightarrow E_1(t+\theta(t)+\tau_1).$$

This composite signal is transmitted over the same communication link to the decryption unit. The decryption unit recovers the phase modulation component, $\theta(t)$, by optically processing the autocorrelation function, $c(\tau)$, of the optical signal, $E_1(t+\theta(t)+\tau_1)$. This process generates an observable interferogram that can be recorded electronically. This is accomplished by applying the same longitudinal path temporal optical delay, $\tau_2 = \tau_1$, or equivalent optical phase shift, onto the received optical reference signal, $E_2(t)$, as performed by the encryption unit on E_1.

$$E_2(t) \rightarrow E_2(t+\tau_2).$$

The autocorrelation function is then obtained by simply interfering the optical signal $E_1(t+\theta(t)+\tau_1)$ with $E_2(t+\tau_2)$

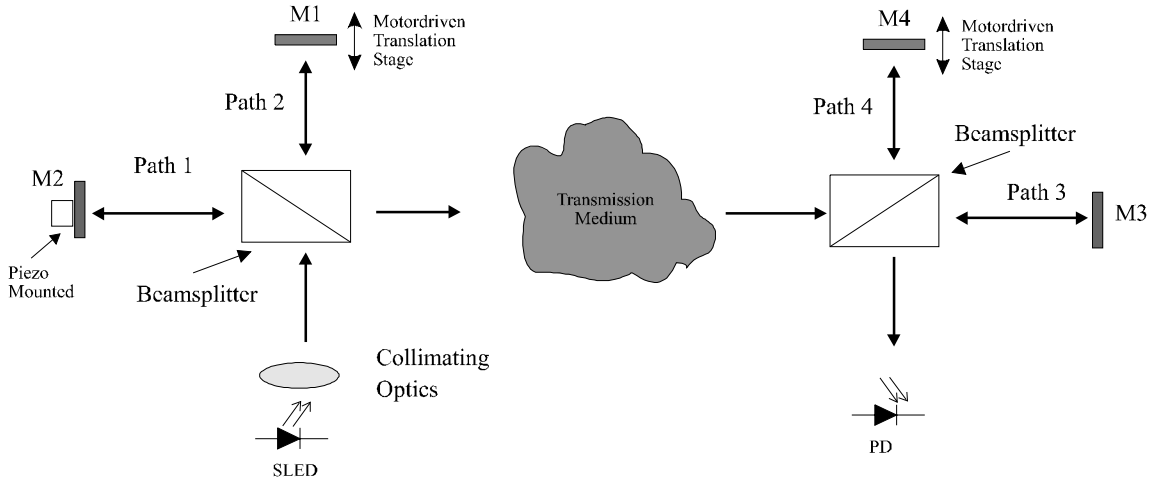
$$c(\tau_2) = \int_{-\infty}^{+\infty} E_1(t+\theta(t)+\tau_1)\cdot E_2(t+\tau_2)dt\,.$$

This process generates the autocorrelation function or optical interferogram of the signal spectrum at the receiving photodetector. By maintaining $\tau_2 = \tau_1$, the data phase modulation, $\theta(t)$, present on the encrypted optical signal, E_1, causes an intensity modulation to appear during this interferometric recombination process. It is this resulting intensity modulation that is recorded to recover the original data that applied the phase modulation at the encryption unit.

The presence at the encryption and decryption units of identical longitudinal path delays, $\tau_2 = \tau_1$, or equivalent phase shifts, determines whether coherent optical interference between the two signals will occur and the existence of a detectable autocorrelation function. Therefore the longitudinal path delay τ_1, or equivalent optical phase shift, at the encryption unit, defines the optical encryption key. In the absence of the correct optical decryption key, $\tau_2 \neq \tau_1$ within the decryption unit, the encrypted optical signal containing the data phase information is indistinguishable, for example, from a broadband signal source, or an amplified optical noise source. The signals, E_1 and E_2, are transmitted over the

same communication link, but with a relative delay. Provided this delay is not greater than the periodicity of any turbulence or distortions on the communication link, both signals experience an identical transmission path.

The bulk optic tandem interferometer arrangement in Figure 1 demonstrates a simple practical realisation of the Optical Field Encryption technique.



$$M2 = \theta(t) \qquad Path\,1 + Path\,3 = \tau_1 \qquad Path\,2 + Path\,4 = \tau_2$$

Figure 1 Encryption-Decryption System realised using bulk optics in free space.

The fiber optic equivalent arrangement is depicted in figure 2.

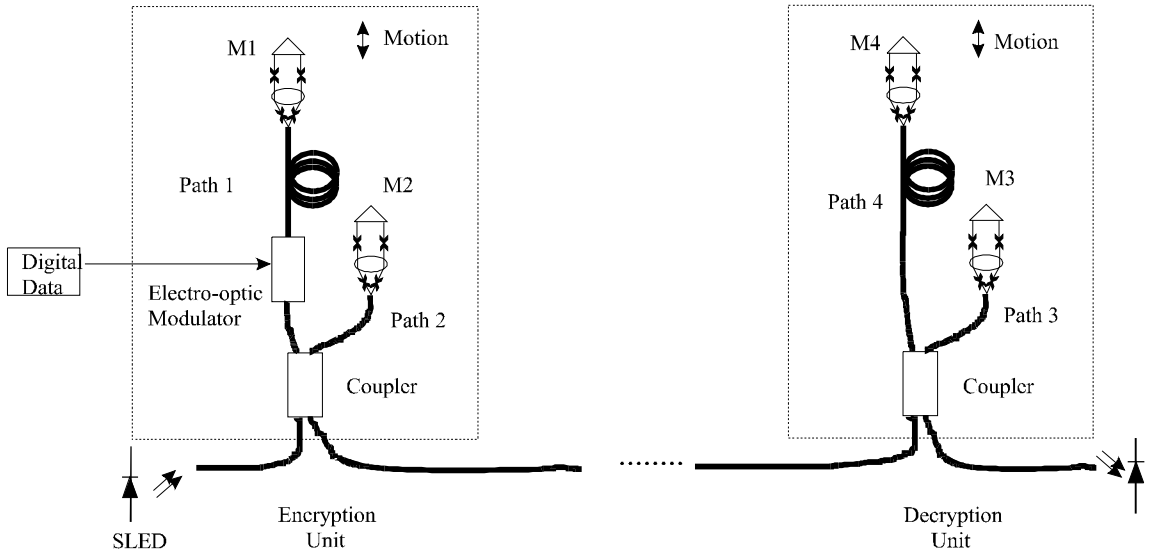


Figure 2 Encryption-Decryption System realised using fiber optic components.

The parameters required to design the above optical field encryption system can be taken directly from the theoretical derivations of other disciplines employing white light interferometry [8,9]. To observe an interferogram the difference between delay paths τ_1 and τ_2 must be less than the coherence length of the source. The coherence length of an optical

source with a Gaussian spectral profile can, to a first approximation, be calculated from (1) and is tabulated in table 1 for the major optical transmission windows for a 40nm broad optical source,

$$\Delta\ell \approx \frac{\lambda^2}{\Delta\lambda}. \qquad (1)$$

Transmission Window	Coherence Length (microns)
780nm	~ 15
1310nm	~ 43
1550nm	~ 60

Table 1 Broadband source coherence lengths.

3. EQUIPMENT

The set-up in figure 1 was realised using standard telecommunications components at 1550nm. The transmission medium was initially a free space length of 1 metre on an optical bench , but was subsequently replaced by 30m of optical fiber, conforming to ITU G652 , a 15dB attenuator and an Erbium Doped Fiber Amplifier providing 25dB gain.

The Encryption and Decryption units employ the same elements except the SLED is replaced by a photodiode at the decryption unit and the encryption unit has one mirror mounted on a low voltage piezoelectric transducer element. This mirror mounting arrangement allows the electronic data source to phase modulate the optical signal, $\theta(t)$).

Amplitude division of the signal was implemented with anti-reflection coated cube beamsplitters of R:T ≈ 45:45 % at 1550nm. Front Surface Mirrors specified to a flatness of lambda/4 at 635nm were employed. The motor driven translation stage, M1, was arbitrarily positioned longitudinally but collinear with the path of the source's output beam. The translation stage in the decryption unit, M4, was actively locked through intensity detection of the interferogram envelope peak by the photodetector, PD, to provide the same path length over paths 1 and 3 as over paths 2 and 4 to an accuracy of 50nm. The piezoelectric transducer that mirror M2 was mounted on, provided a displacement of 3μm for a drive voltage of 100V. The requirement here was for a maximum displacement of 0.75μm, the width of one fringe in the interferogram of figure 4. Detection and storage of the decrypted transmitted data was attained using a prepackaged PIN photodiode, PD, interfaced to a computer through a Data Acquisition Card.

This set-up can easily be enhanced to provide higher modulation rates by replacing the piezoelectric driven mirror with an in-line bulk phase modulator and the pre-packaged photodiode with a high speed photodetector. To protect against scanning of the encryption key by an external laser, an isolator, and if necessary an optical filter, can be placed at the exit and entrances of the encryption and decryption units respectively.

4. RESULTS

The optical source employed was a Super Luminous Light Emitting Diode with a nominal centre wavelength at 1558nm and a FWHM bandwidth of 40nm. The measured spectrum is shown in figure 3 compared to a theoretical Gaussian profile.

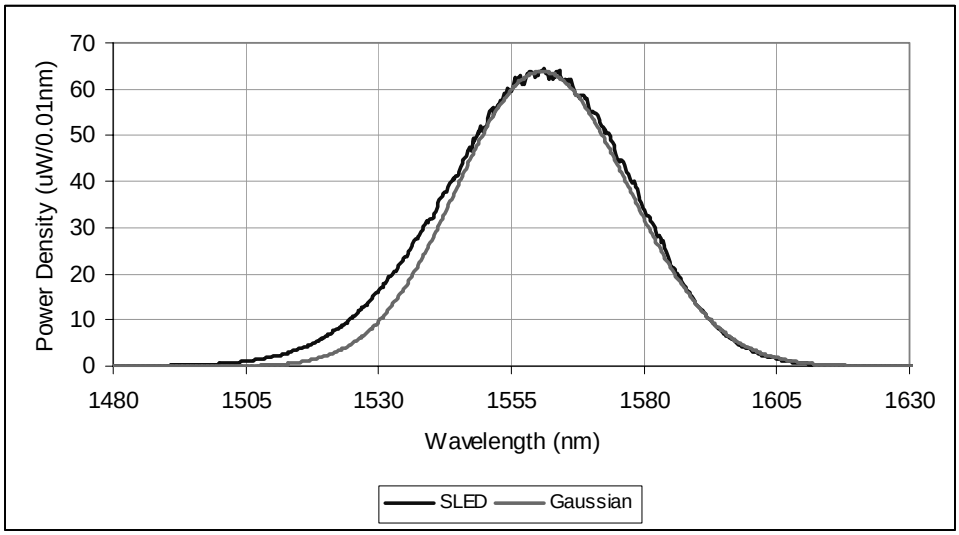


Figure 3 Measured SLED spectrum compared to Gaussian profile.

Scanning the path τ_2 at the decryption unit with respect τ_1 yields the longitudinal coherence function of the SLED source employed at the encryption unit as illustrated by figure 4.

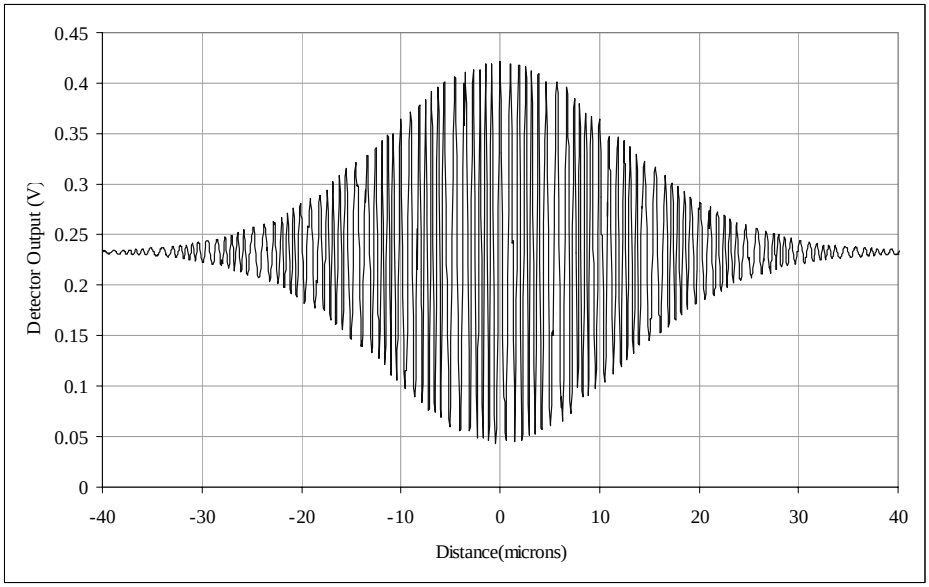


Figure 4 Source spectra and coherence function showing close to 82% visibility.

This shows the high visibility (82%) and definition of the interferogram measured using a translation stage with a minimum step size of 50nm for the zero path difference case (i.e. the autocorrelation function of signal E_1 is generated simultaneously, but independently with the autocorrelation function of E_2 employing a balanced Michelson Interferometer, Path3 = Path4, to intercept the two signals, the two resulting interferograms, originating from Path1 and Path2, intensity distributions summing together but all data phase information, $\theta(t)$, is lost).

Figure 5 shows a 1kHz electrical modulated data waveform prior to optical encryption. This signal is used to phase modulate the optical signal in one arm of the encryption unit by amplitude modulation of the drive voltage applied to the piezoelectric element driving mirror M2, figure 1

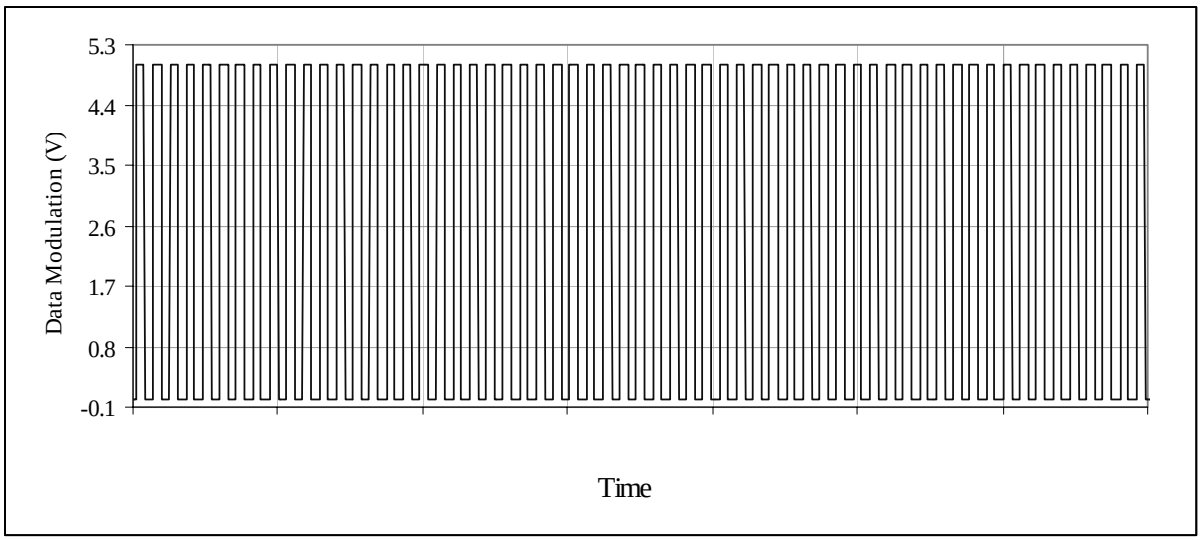


Figure 5 Data Modulation Waveform applied to M2 in figure 1.

Figure 6 shows the corresponding recorded modulated waveform at the optical receivers electrical output of the signal in figure 5 after undergoing optical encryption, transmission and optical decryption when the correct optical decryption key is employed in the receiver unit.

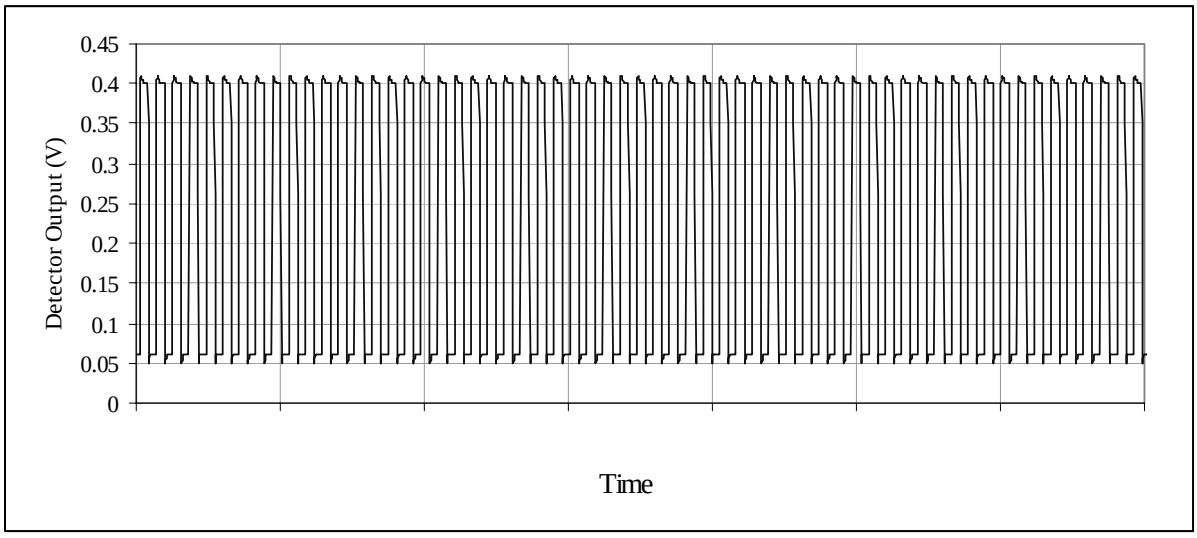


Figure 6 Demodulation waveform recovered after optical decryption.

Figure 7 shows the recorded signal when the incorrect optical decryption key is employed in the receiver unit.

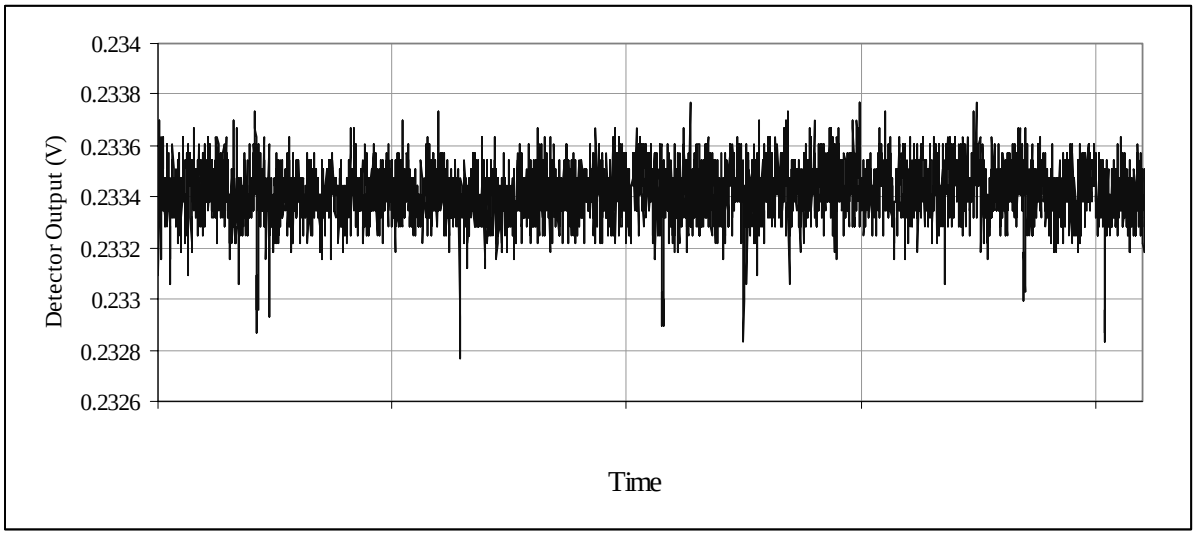


Figure 7 Demodulated waveform obtained with incorrect decryption key.

5. CONCLUSION

An Optical Field Encryption technique realised using standard telecommunication and bulk optical components has been demonstrated. This technique is compatible with fiber optic network component technology and is applicable within all optical spectral transmission windows while offering high data transmission rates. As the data is phase encoded within the encrypted random phase of the optical field of a broadband optical source, decryption must occur instantaneously with the unique hardware key employed at the encryption unit. Otherwise the autocorrelation function and all the necessary optical information to reconstruct it and recover the original data phase modulation information will be lost to an unauthorised observer. The system can be potentially employed for encrypted data transmission, encryption key distribution or as a means of legitimate communication identification.

6. ACKNOWLEDGEMENTS

We would like to thank Scottish Enterprise for the funding and support of this project through their Proof of Concept Programme.

7. REFERENCES

[1] N. Gisin, G. Ribordy , W. Tittel and H. Zbinden, “Quantum cryptography” , Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland
(September 18, 2001; submitted to Reviews of Modern Physics).
[2] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, G. Ribordy, “Quantum Cryptography”, Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland, Received: 29 May 1998, Applied Phys. B 67, 743–748 (1998).
[3] S. Donati, C.R. Mirasso, “Introduction to the Feature Section on Optical Chaos
and Applications to Cryptography”, IEEE Journal Of Quantum Electronics, Vol. 38, No. 9, September 2002.
[4] J. Liu, H. Chen and S.Tang, “Synchronized Chaotic Optical Communications
at High Bit Rates”, IEEE Journal Of Quantum Electronics, Vol. 38, No. 9, September 2002.
[5] Y. Chen and H. F.Taylor, “Multiplexed Fiber Fabry–Perot Temperature Sensor System
using White-Light Interferometry”, June 1, 2002 / Vol. 27, No. 11 / Optics Letters 903.

[6] P. Hlubina, “Dispersive white-light spectral interferometry to measure distances and displacements”, Optical Communications 212 (1-3): 65-70 OCT 15 2002.
[7] T Li, A. Wang, K. Murphy, and R. Claus, “White-Light Scanning Fiber Michelson Interferometer for Absolute Position–Distance Measurement”, April 1, 1995 / Vol. 20, No. 7 / Optics Letters 785.
[8] M. Born and E. Wolf, “Principles of Optics”, Sixth Edition, Cambridge University Press 1997.
[9] E. Hecht, “Optics”, Third Edition, Addison Wesley, 1998.