Defence Science Journal, Vol. 56, No. 2, April 2006 pp. 239-250

Designing Secure and Survivable Stegosystems

S.K. Pal and P.K. Saxena
Scientific Analysis Group, Delhi–110 054

and

S. K. Muttoo
University of Delhi, Delhi–110 007

ABSTRACT

Steganography, the art and science of carrying out hidden communication, is an emerging sub-discipline of information security. Unlike cryptography, steganography conceals the existence of a secret message by embedding it in an innocuous container digital media, thereby enabling unobstrusive communication over insecure channels. Detection and extraction of steganographic contents is another challenge for the information security professional and this activity is commonly known as steganalysis. Recent progress in steganalysis has posed a challenge for design and development of stegosystems with high levels of security and survivability. In this paper, different strategies have been presented that can be used to escape detection and foil an eavesdropper having high technical capabilities as well as adequate infrastructure. Based on the strength and weaknesses of current steganographic schemes, ideas have been progressed to make detection and destruction of hidden information more difficult.

Keywords: Steganography, steganalysis, bit-substitution, transform-domain, undetectability, stegosystem, secure communication, information security, communication security, cryptography

1. INTRODUCTION

For the past many decades, cryptography[1] has been the most reliable mechanism for providing secure communication between the two parties. However, due to the progress in electronic surveillance technology, encrypted traffic can be identified, captured, and disrupted. To ensure that a transmitted signal reaches its destination safely, spread spectrum technology[2] was used for providing unobstrusive communication. These two methods in conjunction formed the basis of communication security for the military and government agencies during wartime and peacetime. In many countries, infrastructure, cost, and bandwidth requirements, combined with problems regarding use of cryptography, have restricted the use of such a scheme by the common man.

Steganography[3] gained importance due to an increasing need for providing secrecy in an open environment like the internet. With observers and adversaries all around, steganography attempts to hide the existence of a message and makes the communication undetectable. Due to the redundancy

Revised 20 September 2004

available in digitised images, audio and video, it is possible to hide a message inside the media (also known as cover) without raising any suspicion regarding its presence. Steganography has enabled the common man to carry out secret communication without the heavy infrastructure and usage restrictions.

Steganography has quite often been compared with cryptography as a mechanism for providing information security. The choice of these two schemes depends on the potential adversaries and the environment in which security is required. Though both of these schemes protect information from unwanted observers, individually neither of these has the potential to provide complete communication security solutions (Table 1). Steganography used in conjunction with cryptography provides an additional layer of information security.

Widespread use (or misuse) of cryptography and steganography is a matter of serious concern for the intelligence and law-enforcement agencies. It is possible to coordinate criminal or unlawful activities over the internet simply by hiding messages using nonstandard stego-algorithms together with encryption. An organisation responsible for controlling cyber-crimes and booking cyber-culprits first needs to establish the existence of hidden communication and then analyse it to extract the meaningful messages.

To control objectionable activities over an open network like the internet, a few security agencies have initiated packet-sniffing[4] and eavesdropping activities based on keyword search or statistical analysis of the traffic. Echelon and Carnivore are two such attempts that have raised serious questions regarding privacy of individuals and secrecy of their communication. Steganography has emerged as a solution to foil this type of eavesdropping.

The potential threats offered by steganography for carrying out criminal activities have once again bothered the law-enforcement agencies, resulting in the creation of expertise and infrastructure related to its monitoring in different countries. With the progress in steganography detection[5], it is now possible in a few cases to identify steganographic contents in digital media. The long-term goal is to extract the hidden bits from an intercepted/captured stego-media and to reconstruct back the message possibly after cryptanalysis.

2. STEGANOGRAPHIC DESIGN ISSUES

Steganography started its journey with simple bit-replacement schemes[6] in the spatial domain for images and video, and in the time domain for audio signals. The basic aim was to replace the noise or statistically-uncorrelated regions of a container with the message bits without degrading the perceptual quality of the media. Desirable characteristics of a steganographic system have been perceptual transparency, message survivability, support for high data rate (also called the capacity) and undetectability.

Table 1. Suitability of steganography and cryptography for secure communication

Steganography	Cryptography
• Makes information imperceptible/ transparent to an observer	• Makes information unintelligible to an observer
• Provides secrecy in open-system environment with active adversaries at an additional cost.	• Does not ensure covertness on the channel. Cost of transmitting an *n*-byte message is lower.
• Does not yet have a definition of practical system security	• Complexity/ security of the system can be quantified
• System is secure if protection mechanism is unknown or hidden information is undetected	• System is secure if secret key is unknown to an adversary. Algorithm is mostly open to public
• In case of successful attack, security can be restored by replacing the entire hiding scheme	• Security can be restored by replacing only the compromised key
• An emerging discipline without rigorous mathematical background	• Well-established field with strong mathematical foundations

Other requirements include usability in real time, simple and low-cost hardware realisation, self-detectability, and system with open algorithm and secret keys.

Steganographic schemes based on hiding data in the spatial domain were simple to implement and computationally inexpensive. Measures based on properties of image palettes, distribution of pixels within a block, luminance, and entropy were used to build systems facilitating high data rate. Such systems were required for secret transmission of pictures, maps, sketches, human speech, and sounds. Stego-media created from these systems, however, could not sustain many forms of attacks, and hence, were not very useful for communication over public networks.

To address the issue of message survivability or robustness, transform-domain information hiding[7,8] systems gained importance. Image steganography systems based on discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT) became popular and could provide a satisfactory trade-off between transparency, message survivability, and capacity. A large number of schemes based on manipulation of the JPEG coefficients were used for hiding data in images[9]. Similarly for audio, steganography in the spectral and cepstral domains was popular[10]. Choice of a suitable workspace became an important factor for the design of secure and survivable stegosystems.

Steganographic systems could be classified into generations[11] based upon perceptual and statistical properties satisfied by the respective stego-objects. Whereas, the first-generation systems were based on simple bit-replacement schemes, the second-generation systems utilised models of human perceptual (visual, audio) system to ensure transparency after data hiding. The third-generation systems, in addition, ensured that the statistical properties of the cover were undisturbed by manipulating the media. The present-generation systems attempt to provide high levels of secrecy by carefully embedding the secret bits (indirectly) in the transform-domain. Perceptual transparency and preservation of first-order statistical properties are assumed by default. Such systems, if properly designed, have been observed to satisfy most of the desirable properties (including undetectability and survivability) of a steganographic system. It is important to note that undetectability of a specific stegosystem is not an everlasting phenomenon and is redefined with the progress in steganalysis.

As in the case of cryptosystems, it was observed that stegosystems too have to be evaluated for implementation weaknesses, and other flaws in their design. Despite strength of the underlying hiding scheme and other precautions, a poor system design could lead to successful attacks by an adversary without much effort.

3. STRATEGIES FOR ESCAPING DETECTION

The present communication scenario assumes the presence of active wardens having the capability of observing and modifying the data transmitted over a communication channel. Secure steganographic schemes, that can resist many types of modifications and tampering, are required. A stegosystems' designer has to ensure that the hiding process smoothly embeds the external data in the digital object without introducing visual degradations and statistical incompatibility. To introduce survivability against attacks, either the secret data has to be replicated (to provide redundancy) or it has to be embedded in the significant coefficients/parameters of a transformed domain without disturbing the fidelity of the media. Though steganographic techniques are not developed to offer robustness to all types of intentional attacks, these should be able to survive common signal distortions and noise in the communication channel or format conversion required by applications at the receiving end.

Secret transmission of pictures, maps, sketches, voice, and sounds is needed in many situations. This requires steganographic schemes that support high data rates. Flipping of the least significant bits (LSBs) or direct bit-replacement techniques used for providing high payload is not acceptable any more. These are vulnerable to message detection using present steganalysis methods. In general, larger the size of the embedded data, higher is the chance of its detection. Therefore, a stegosystems'

designer has to address the security aspects from a broader angle while designing a high-capacity stegosystem.

Embedding smaller messages offer immunity to many side effects, many of which are unknown at the time of designing a steganographic scheme. Current progress in steganalysis of images does not mean that high capacity secure steganography is not possible. A number of domains are available that promise a respectable payload together with message survivability and undetectability. Ways to escape detection under different scenario have been explored while retaining the other desirable properties in a stegosystem.

3.1 Bit-replacement Steganography: Alternate Strategies

Direct bit-substitution steganography has been successfully analysed by a number of researchers. Except for very low embedding rates, these systems are, in general, detectable. However, there are safer ways for message hiding using these schemes. It has been observed that instead of bit-replacement, minor increment or decrement of the coefficient values in a particular domain provides safer steganography.

Accuracy of steganalysis schemes also depends upon concentration of the hidden message. Some of these methods fail if the message is randomly scattered, whereas others give poor results if the message is sequentially placed in a local area of an image. To foil detection by LSB steganalysis, conditional embedding may be performed. The RS steganalysis[12] scheme quantifies the regularity or smoothness of a group of pixels and defines regular (*R*), singular (*S*) and unusable (*U*) pixel groups. By analysing the *R* and *S* groups, one can get an idea of the length of the embedded message in the LSB plane. To escape or foil RS steganalysis, one can embed a bit in the LSB of a pixel only if its difference with the immediately surrounding pixels is more than two.

Similarly, instead of hiding data uniformly, it is safer to embed data in specific regions of an image using a complexity/quality measure. This is shown in Fig. 1, where 4 x 4 blocks have been marked according to their randomness. An entropy-based measure[13] was used to find suitable LSB regions for data hiding. The statistically complex regions are shown in lighter shades in Fig. 1(b), whereas the black regions have minimum entropy and should not be modified. Figure 1(c) shows the complexity histogram of the image blocks. The sorted entropy graph in Fig. 1(d) helps to decide the amount of data to be embedded and the corresponding blocks to be selected for embedding. Higher the randomness of the media used for data hiding, more is the embedding capacity. Therefore, treatment of all covers alike is not desirable in steganography. The size and nature of a cover should, in turn, dictate the maximum size of a message to be embedded.

In a natural image, adjacent bit-planes are correlated. LSB embedding may invite steganalysis based on statistical analysis of blocks taken from the immediate higher planes, eg, the 7th bit-plane. To escape detection, one needs to make the higher planes correlated with the modified LSB plane.

3.2. Parameter Encoding

A number of stego-schemes have been designed that partition a cover into blocks or frames, use a measure to decide the suitability of each block for data embedding (optional), and ultimately replace the contents of a suitable block with the secret message bits, thus providing high-capacity steganography. Some designers do not replace the entire contents of the cover block but embed a bit as a function of selected pixels/samples in the block. An example is hiding in the parity of a set of pixels. Another efficient method for information hiding is by incorporating slight modifications in the compression algorithm. This has been achieved for the JPEG, MPEG still and moving picture standards, and singular value decomposition (SVD)-based schemes.

Undetectable schemes can be designed by transforming the cover blocks to another domain and then hiding a bit by manipulating the coefficients of the transform-domain. A few such schemes are: (a) hiding in the JPEG coefficients of an image by swapping almost equal magnitude values, (b) hiding by encoding a message in the coefficients of an

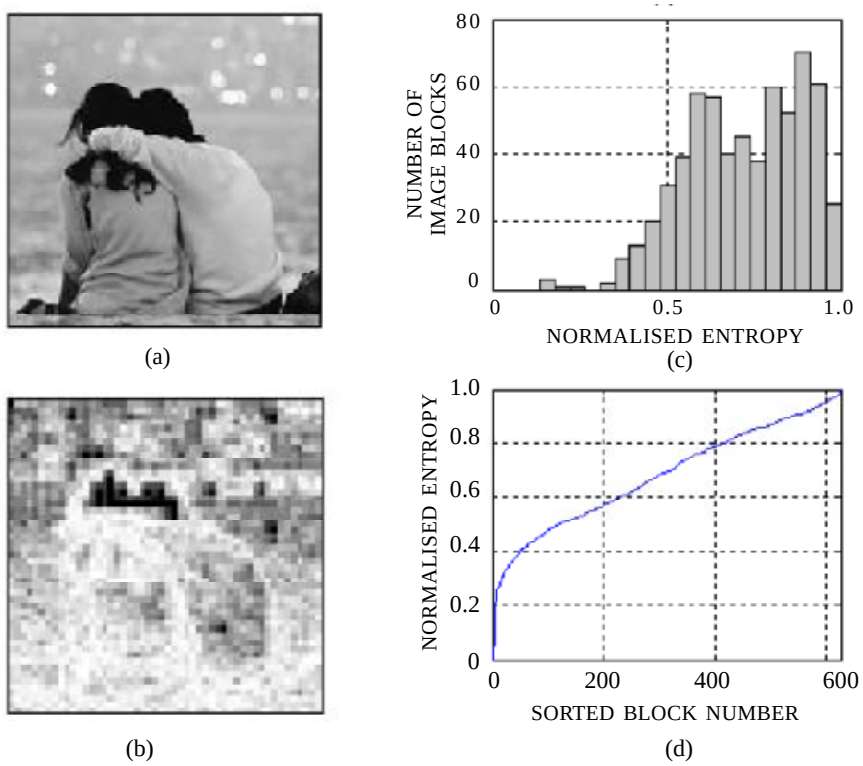


Figure 1. Suitability of local regions for data-hiding: (a) original image, (b) entropy of 4 x 4 blocks, (c) histogram of normalised entropy and (d) sorted entropy graph.

affine transform, (c) hiding in the SVD-domain of an image by slightly modifying the SVD coefficients, (d) hiding in the cepstral-domain of a speech signal by enforcing some statistical parameters to represent a bit (0 or 1) of the secret message, and (e) hiding bits in the LPC parameters derived from a speech frame. These methods are better than direct substitution methods in terms of survivability, transparency, and undetectability.

The scope of designing stego-systems using different media transforms was explored. Let X_S and represent the cover and stego blocks of a digital media. Then in generic terms

$$X_S = \Im^{-1}(\aleph(\Im(X_C),\mu,k)) \quad (1)$$

where $\aleph$ is the embedding process, μ is the hidden message, k is the secret key, $\Im$ and $\Im^{-1}$ are the direct and inverse transforms on a block. The first option is hiding a message directly in the coefficients of a transform. The other option is to encode bits in the parameters controlling a transform. Such systems can be represented by

$$X_S = \Im_\alpha^{-1}(\aleph(\Im_\alpha(X_C),\mu,k)) \quad (2)$$

where α represents the parameter(s) of the transform $\Im$. A number of such domains are available for images, audio, and video and can be efficiently exploited for steganography. Geometrical transformations like the affine, projective, and polynomial transforms can be applied to images or parts of an image by varying the set of associated parameters. A stegosystem based on 2-D geometrical transform has been described in which a transformed pixel (x'y') is represented by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} \quad (3)$$

with the parameter set $\alpha = \{a,b,c,d,e,f\}$. A bit-stream can be converted into the coefficients of a particular transform by defining a suitable range and quantising it into intervals. The number of bits that can be embedded into a parameter is dependent upon the quantisation size and length of range for that parameter. It is important to ensure that the

chosen range does not affect the transparency of the media. By increasing the quantisation size of a parameter, it is possible to improve survivability against attacks at the cost of capacity.

Stegosystems based on these transforms have been found to be survivable against many signal processing operations and lossy format conversion. However, the schemes described in this sub-section require the availability of a cover media with the receiver to extract the secret message. Despite practical shortcoming associated with *a-priori* sharing of cover media, steganalysis of such schemes is not easy and has also not been reported in the literature. In the following sub-sections using self-detectable steganographic schemes, an authorised receiver can extract the secret message from the stego-media only and does not require the cover media used by the sender.

3.3. Secure Schemes for JPEG Images

JPEG is today one of the most popular coding formats for still images. Data hiding in JPEG images is performed in the discrete cosine transform (DCT)-domain and is considered to be superior in terms of transparency and robustness compared to many direct spatial-domain methods. However, steganalysis of some of these systems has been possible due to a number of reasons. It was shown[14] that images previously stored in JPEG format show typical characteristics due to quantisation introduced by JPEG compression. Even a few external bits can make the image incompatible with the JPEG format, thus providing clues for detection. In such cases, compatibility and not capacity plays a role in stego-detection.

Certain assumptions in designing steganographic schemes have quite often helped in steganalysis of these systems. Many designers have assumed that the distribution of pixels in images follow a Gaussian distribution. Similarly, coefficients in the transform-domains are also assumed to have Gaussian distribution. Therefore, it was thought to be safe to replace these coefficients by zero-mean white Gaussian distributed signal or simply by an encrypted message.

It is now gradually realised that distribution of coefficients in a number of domains is not Gaussian. A simple example is the DCT coefficients that deviate from a Gaussian distribution to an extent that may be exploited by a steganalyst. It has been possible to get clues regarding hidden messages by looking at the histogram of DCT coefficients and its first-order differences. Discontinuities introduced in the sub-block boundaries due to embedding also serve as an important clue to the steganalyst.

Therefore, while designing a secure JPEG-based scheme, one has to bear in mind that all the decoded blocks are JPEG-compatible. This can be done using a table of quantised coefficients and modifying only a few coefficients per block. Next thing to keep in mind is that the compatibility of the external data with the coefficients has to be ensured. This may require first-and higher-order statistical analysis of the stego-image. Finally, one needs to examine for peculiarities by arriving back to the initial spatial domain that might have been unknowingly introduced by manipulations in the transformed domain. These precautions help to foil the detection of hidden messages in a digital image.

3.4. Histogram-preserving Techniques

Well-designed steganographic algorithms try to preserve perceptual as well as statistical properties of a cover in the corresponding stego-object. The idea of preserving the histogram of an original medium in a stego-medium was initially implemented and demonstrated for the stego-tool, Outguess. After data embedding, a designer may process a stego-image by modifying the spare coefficients so that the histogram of DCT coefficients for the stego-medium (nearly) matches that of the cover. There have been attempts to design histogram modification schemes that minimise the mean squared error between the input and output data or the object. Steganographic systems based on histogram preserving data mapping (HPDM) were proposed by Eggers, Bauml, and Girod[15], that maintain zero relative entropy between a cover and its corresponding stego-object.

It is obvious that a steganalyser for systems like Outguess has to exploit criteria other than the coefficient histograms. Histogram-preserving methods, however, do not ensure preservation of all other statistical properties. It was observed that enforcing the first-order statistics to a target distribution might give rise to unexpected signatures in a stego-media. Fridrich[16], *et al.* could find discontinuities in the boundaries of JPEG blocks as a peculiar property for detection and message size estimation.

By manipulating the first-order statistics of a stego-object, it may not always be possible to fool a steganalyser whose analysis is based on higher-order statistical features. As a countermeasure, it was suggested[11] to preserve higher-order statistics in the design of stego-systems. Farid's steganalysis[17] could not directly detect the presence of messages embedded using the histogram-preserving method. The HPDM method could preserve statistics related to sub-band coefficients. However, the statistics related to log error produced by an optimal predictor could not be retained. In turn, by modifying the mapping process to neglect the DCT values –1, 0, and 1, the prediction error histogram could also be retained. Thus, the clue that a steganalyst would have used for message detection could be foiled using this simple scheme.

3.5. Adaptive Steganography

There may be situations where the communicating party is able to gain some knowledge regarding the warden's steganalysis capabilities. This knowledge could be used for: (i) adapting the stego-algorithm to escape detection from the warden's steganalysis technique, and/or (ii) achieving higher embedding capacity while maintaining undetectability. Chandramouli[18] visualised the following situations for practicing adaptive steganography:

- Using a scheme that the warden's steganalyser cannot detect
- Restricting the number of bits to be embedded
- Embedding in statistically-complex regions
- Post-processing a stego-object to confuse the warden's steganalyser.

A random LSB embedding steganographic scheme was analysed using the detection methodology proposed by Dumitrescu[19], *et al*. Their method described below is based on statistics of local pixel regions that change due to LSB embedding. It was then shown that hidden communication may be carried out even when the warden is using the specific detector mentioned above.

An image is partitioned into pairs of horizontal adjacent pixels. This set was called as P and it defines *subsets* X and Y of P as follows:

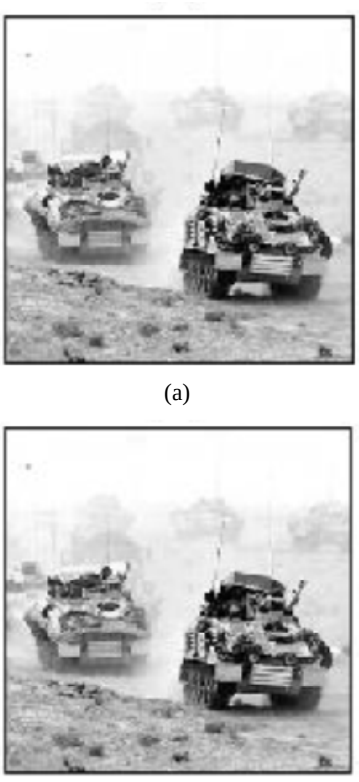
Let $(u,v) \in P$. Then $(u,v) \in X$ if v is even and $u < v$ or v is odd and $u > v$.

Also $(u,v) \in$ Y if v is even and $u > v$ or v is odd and $u < v$.

For a natural image, it was found that $|X| = |Y|$, since the gradient of intensity function in any direction has equal probability to be positive and negative. Z was defined as $(u,v) \in Z$ if $u = v$. The set Y is further partitioned into two *subsets*, W and V so that $(u,v) \in W$ if (u,v) is of the form $(2k, 2k + 1)$ or $(2k + 1, 2k)$ and $V = Y -$ W. Then $P = X \cup W \cup V \cup Z$ is the union of these primary sets.

In case of LSB embedding as shown in Fig. 2, for the pair (u,v) it is possible that: (i) neither u nor v is modified, (ii) only u is modified, (iii) only v is modified, or (iv) both u and v are modified. These modification patterns are represented by 00, 01, 10, and 11 with 1 indicating LSB-reversed samples and 0 indicating intact samples.

Any pixel pair modified by a specific pattern changes its set membership and the set migration relationship is obtained as shown in Fig. 3. An arrow drawn from set A to set B and marked with a modification pattern indicates that a pixel pair of A becomes a pair of B if modified by the marked pattern. For each modification pattern $\pi = \{1, 2, 3, 4\}$ explained earlier and any subset $A \subseteq P$, denote by $\rho(\pi, A)$ the probability that the pixel pairs of A are modified under the pattern π. It was assumed that the message bits are randomly scattered in the message space independent of image features. If p denotes the ratio of the message length in bits



(a)

(b)

Figure 2. LSB message embedding: (a) original image and (b) image with modified LSB plane.

to the total number of pixels, the fraction of pixels modified by the LSB embedding operation is $p/2$. Then from the conditions (i)-(iv) and the set migration diagram, $\rho(1, P) = (1 - p/2)^2$, $\rho(2, P) = \rho(3, P) = p/2.(1 - p/2)$ and $\rho(4, P) = (p/2)^2$. The cardinalities of $A' \in \{X', Y', V', W', Z'\}$ after message embedding can be obtained from the stego-image.

After solving a set of equations based on $|X'|$, $|Y'|$ and $\gamma = |W' \cup Z'|$, one obtains

$$0.5\gamma p2 + (2|X'| - |P|)p + |Y'| - |X'| = 0$$

Details of this derivation are given by Dumitrescu[19], *et al*. The value of p is obtained by solving the above quadratic equation. Figure 4 shows the sets X, Y, and Z obtained for the previous natural image C as well as the stego-image S. For a natural image, statistically $|X| = |Y|$. The difference in the relative magnitudes of these sets [shown in Fig. 4(b)] indicates the presence of a hidden message.

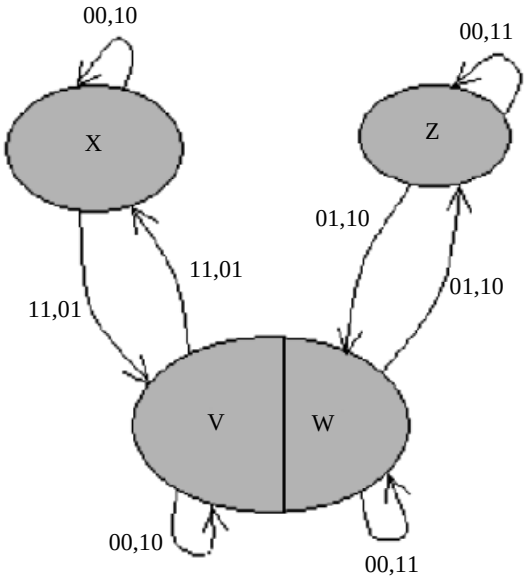


Figure 3. Set migration relationship for LSB message embedding.

In the remaining sub-section, different means of adapting the algorithm are discussed for carrying out steganography in the presence of the warden. The simplest way is to use a bit-plane other than the LSB image plane. However, such a scheme is not useful as the underlying assumptions regarding the warden's steganalyser are too strong to be practical.

Apart from sharing the secret key, the sender and the receiver may also share a predecided strategy (may be a code) to avoid detection. The algorithm may embed bits in the noisy regions of the image

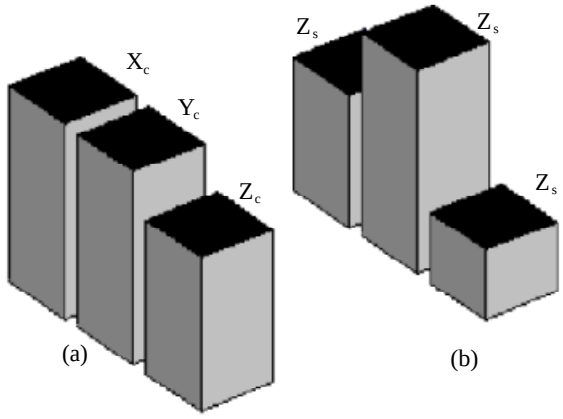


Figure 4. Detection sets for (a) cover and (b) stego-image

where it becomes difficult to perform analysis based on statistical tests. In a normal image, it has been observed that the blocks with the highest variance are normally 5-20 per cent of the cover size. A stego-designer may select these blocks, mark these, and hide one or more bits in the coefficients derived from these blocks. These statistically complex blocks were used to embed message bits and it was found that the cardinalities of the detection sets did not reflect the presence of hidden data.

Another method is to do some form of post-processing on the stego image to dilute the aftereffects of data embedding. By adding zero-mean noise to the regions not containing the secret bits, it was possible to increase the probability of detection error and to confuse a steganalyst. Noise may also be introduced in the coefficients or parameters controlling a transformation.

3.6. Data Masking for Improving Capacity

To achieve robustness, transparency, and undetectability, modern steganographic schemes have to compromise with the payload. Data masking[20] is an attempt to provide channel capacity higher than conventional steganography with the ability to foil an eavesdropper using statistical analysis tools to detect and capture secure channels. It uses techniques to mask an encrypted message and makes it appear like a normal multimedia object to a warden monitoring the channel. The generic block diagram for data masking is depicted in Fig. 5. This method can also be used to provide covertness to the encrypted contents hidden inside a cover (though the capacity will be reduced). The disadvantage of using data-masking techniques is that their purpose may be defeated if the eavesdropper uses perceptual tests for analysing the traffic.

Methods that can convert an encrypted stream into a more correlated signal before transmission are considered for reconstructing the signal at the receiving end. One way is to use an inverse Wiener filter. Also by performing linear predictive coding (LPC)-based analysis/synthesis, the inverse of LPC analysis filter is used to convert an encrypted

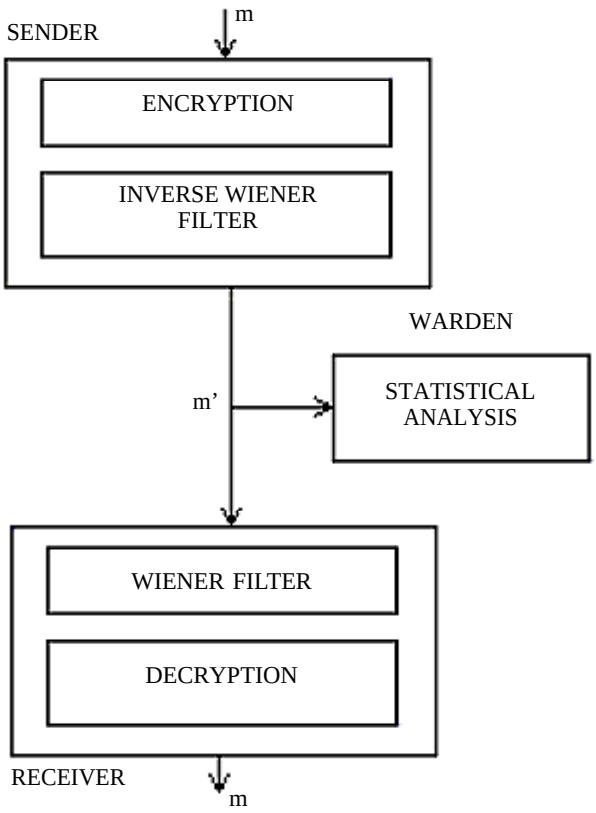


Figure 5. Generic block diagram for data masking

stream to a waveform resembling an audio signal. This is shown in Fig. 6. The filter coefficients are transmitted with each audio frame. On the receiving side, the encrypted stream is reconstructed and decrypted to get back the meaningful message. These schemes are not robust and need substantial improvement to be able to foil active wardens.

The classical definition of steganography emphasised only on the statistical aspects without considering the perceptual criteria. The perceptual criteria come into picture mostly when a human warden is involved. Present-day automated tools (for analysis of broadband traffic) face bandwidth problems for handling packets in real time and also do not have the perceptual judgment capability that human beings have. Due to these practical limitations (for realisation of a perfect warden), data masking has the potential for high capacity secret communication under the present scenario.

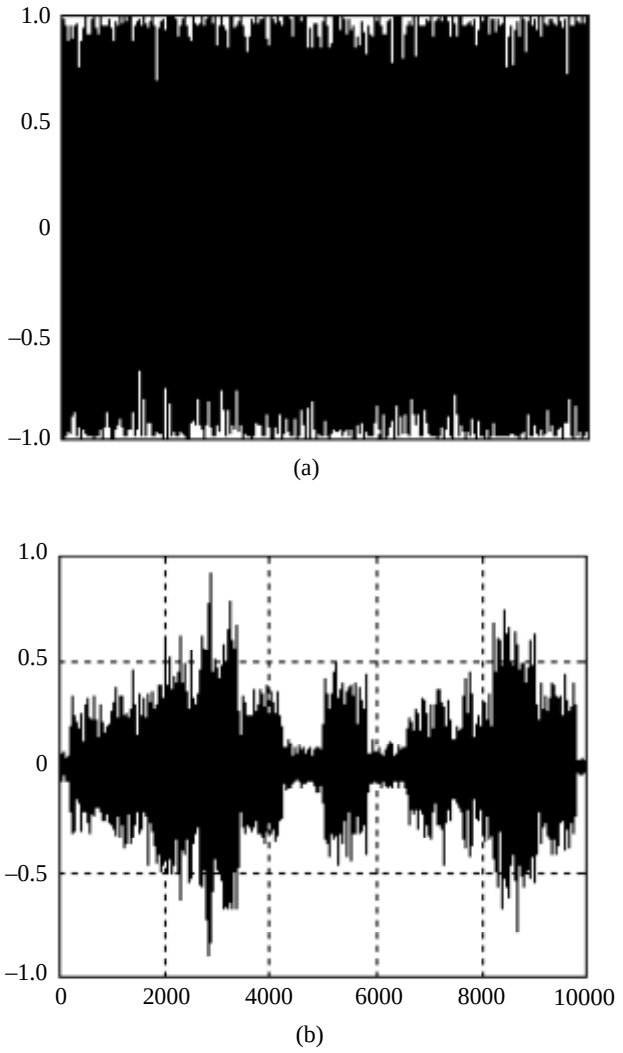


Figure 6. Conversion of: (a) encrypted message to (b) more correlated (speech) signal.

4. CONCLUSION

The study focuses on improving the design of steganographic systems based on the current steganalysis scenario. Different ideas have been presented for carrying out hidden communication over public channels prone to passive and active attacks. Schemes for improving undetectability and survivability have been presented to ensure that the secret message reaches its authorised receiver without obstruction and modification. Experimental results have shown the feasibility of practicing steganography safely even in the presence of smart and powerful wardens.

5. FUTURE TREND

Future R&D includes design of stego-systems for wireless ad hoc networks where higher levels of security and message survivability are required. In addition, automatic removal of hidden messages and restoration of the original media used in steganography are also the future trends of study.

REFERENCES

1. Rhee, M.Y. Cryptography and secure communication. McGraw Hill Co, Singapore, 1994.

2. Pickholtz, R.L.; Schilling, D.L. & Milstein, L. B. Theory of spread spectrum communications: A tutorial. *IEEE Trans. Comm.*, 1982, **30**(5), 855-84.

3. Petitcolas, F.; Anderson, R. & Kuhn, M. Information hiding-A survey. *Proceedings IEEE*, 1999, **87**(7), 1062-078.

4. Fisch, E.A. & White, G.B. Secure computers and networks: Analysis, design and implementation. CRC Press, 2000.

5. Provos, N. & Honeyman, P. Detecting steganographic contents on the internet. *In* Proceedings of the Network and Distributed Systems Security Symposium (NDSS), 2002.

6. Wang, R.Z.; Lin, C.F. & Lin, J.C. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*, 2001, **34**, 671-83.

7. Cheng, Q. & Huang, T. S. An additive approach to transform-domain information hiding and optimum detection structure. *IEEE Trans. Multimedia*, 2001, **3**(3), 273-84.

8. Alturki, F. & Mersereau, R.M. Secure blind image steganographic technique using discrete Fourier transformation. *Proceedings of the IEEE Inter Conference Image Processing*, October 2001, Thessaloniki, Greece.

9. Provos, N. Outguess-universal steganography. http://www.outguess.org.

10. Pal, S. K. & Saxena, P. K. Secret communication using voice and music. *In* Proceedings of the 6th International Workshop on Recent Trends in Speech, Music and Allied Signal Processing (IWSMSP-2001), 2001, New Delhi.

11. Pal, S.K.; Saxena, P.K. & Muttoo, S.K. A systematic approach to steganalysis of images. *In* Proceedings of the Pacific Rim Workshop on Digital Steganography (STEG'02), 2002, Kitakyushu, Japan. pp. 179-88.

12. Fridrich, J. & Goljan, M. Practical steganalysis of digital images- state-of-the-art. *In* Proceedings SPIE Photonics West 2002: Electronic Imaging, Security and Watermarking of Multimedia Contents, Vol. IV, 4675, January 2002. pp. 1-13.

13. Droogenbroeck, M.V. & Delvaux, J. An entropy-based technique for information embedding in images. *In* Proceedings of the 3rd IEEE Benelux Signal Processing Symposium, March 2002, Leuven, Belgium. 2002.

14. Fridrich, J.; Goljan, M. & Du, R. Steganalysis based on JPEG compatibility. *In* SPIE, Special Session on Theoretical & Practical Issues in Digital Watermarking and Data Hiding, SPIE Multimedia Systems and Applications IV, Denver CO, August 1998, **4518**.

15. Eggers, J.J.; Bauml, R. & Girod, B. A communication approach to image steganography. *In* Proceedings of SPIE: Security and Watermarking of Multimedia Contents IV, San Jose CA. **4675**. 2002.

16. Fridrich, J.; Goljan, M. & Hogea, D. New methodology for breaking steganographic techniques for JPEGs. *In* SPIE Electronic Imaging 2003, Security and Watermarking of Multimedia Contents, 2003, Santa Clara, California.

17. Farid, H. & Lyu, S. Detecting hidden messages using higher-order statistics and support vector machines. *In* Proceedings of the 5th Workshop on Information Hiding, 2003, LNCS 2578, Springer-Verlag, Berlin Heidelberg.

18. Chandramouli, R. & Memon, N. Adaptive steganography. *In* Proceedings of the SPIE Conference on Security and Watermarking of Multimedia Contents, 2002.

19. Dumitrescu, S.; Wu, S. & Wang, Z. Detection of LSB steganography via sample pair analysis. *In* 5th Information Hiding Workshop, October 2002, Noordwijkerhout, Netherlands, LNCS 2578, Springer-Verlag.

20. Radhakrishnan, R.; Shanmugasundaram, K. & Memon, N. Data masking: A secure covert channel paradigm. MMSP-2002, US Virgin Islands.

Contributors

Mr S.K. Pal did his postgraduation in Computer Science from the J. K. Institute of Applied Physics, Electronics & Communications, University of Allahabad in 1990. He joined DRDO at the Scientific Analysis Group, Delhi, in 1991 and is presently working as Scientist D. His research interests include: Digital signal processing, cryptology, multimedia and network security, information hiding and soft computing. He has worked on projects related to speech processing, communications and cryptology. He has about 40 publications to his credit and is a member of several scientific and technical societies.

Dr P.K. Saxena did his MSc in Mathematics from the Christ Church College, Kanpur, in 1971 and PhD for his work on radical theory of near-ring (Algebra) from the Indian Institute of Technology (IIT), Kanpur, in 1978. He joined DRDO in 1981 and is presently Scientist G and Director,Scientific Analysis Group. He has published approx. 50 research papers in national and international journals and written around 40 technical reports. He has headed DRDO projects and also guided many BE/ME students on their industrial training projects. He has refereed many papers for national and international journals. His areas of research include: Cryptology, fuzzy logic, algebra, artificial intelligence, genetic algorithms, and speech technology.

Dr S. K. Muttoo obtained his PhD from the University of Delhi in 1982. He also did MTech from the IIT, Kharagpur, in 1990 and joined the Department of Computer Science, University of Delhi as Reader in 1991. His areas of specialisation include: Coding theory, information security, and cryptography. He has published several papers in various national/international journals and is a life member of the Computer Society of India.