ISSN:0975-9646

Data Hiding in Audio by Reserving Room in Advance of Encryption

B.Kavitha[1], Mrs.Brindha Rajakumari[2]

[1]PG Scholar CSE Dept., Bharath University,
Chennai, Tamil Nadu, India
[2]Asst. Professor, CSE Dept, Bharath University,
Chennai, Tamil Nadu, India

***Abstract*— Data hiding was done using plain text, still images, video and IP datagram for a lengthy era .In recent time's audio steganography is spot of heart. This manuscript presents an original method of top secret data to be unseen in acoustic by means of cryptography and steganography collectively. The protection of this method is enhanced by using of an encryption method prior to the data embedding step. First data is scientifically encrypted, then RSA encryption is applied on it. Resultant data is fixed in audio. The perceptual excellence of the host audio signal was not to be degraded while embedding. This paper supports different formats of wav audio such as 16 bit and 8 bit .wav audio, mono and stereo .wav audio irrespective of its sampling frequency22 kHz or 44 kHz. The intend of this project is information mining and audio data with no fault in the Encrypted audio signals. This development ensures that full improvement of information and acoustic information.**

Keywords—Information Hiding; Encryption; Frequency 22; Acoustic Information; Steganography

I. INTRODUCTION

Data hiding in audio signals is especially challenging, because the Human Auditory System (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than thousand to one. Sensitivity to additive random noise is also acute.

The perturbations in a sound file can be detected as low as one part in ten million which is 80dB below ambient level. However there are some 'holes' available. While the has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out the quieter sounds.

Additionally, the HAS is unable to perceive absolute phase, only relative phase. Finally there are some environmental distortions so common as to be ignored by the listener in most cases.

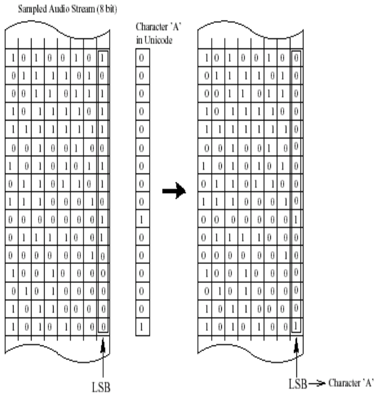
LOW-BIT ENCODING:

Low-bit encoding is the one of the simplest way to embed data into other data structures. By replacing the least significant bit of each sampling point by a coded binary string, we can encode a large amount of data in an audio signal.

Ideally, the channel capacity is 1 kb per second (kbps) per 1 kilohertz(kHz), e.g., in a noiseless channel, the bit rate will be 8 kbps in an 8 kHz sampled sequence and 44 kbps in a 44kHz sampled sequence. In return for this large channel capacity, audible noise is introduced. The impact of this noise is a direct function of the content of the host signal, e.g., crowd noise during a live sports event would mask low-bit encoding noise that would be audible in a string quartet performance.

Adaptive data attenuation has been used to compensate this variation. The major advantage of this method is its poor immunity to manipulation. Encoded information can be destroyed by channel noise, re-sampling, etc., unless it is encoded using redundancy techniques.

In order to be robust, these techniques reduce the data rate which could result in the requirement of a host of higher magnitude, often by one to two orders of magnitude. In practice, this method is useful only in closed, digital-to-digital environments.



1	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0	0
0	1	1	1	1	0	1	0	0	0	1	1	1	1	0	1	0
0	0	1	1	0	1	1	1	0	0	0	1	1	0	1	1	0
1	0	1	1	1	1	0	1	0	1	0	1	1	1	1	0	0
1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0
0	0	1	0	0	1	0	0	0	0	0	1	0	0	1	0	0
1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	0
0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	0
1	1	1	0	0	0	1	0	0	1	1	1	0	0	0	1	0
0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1
0	1	1	1	1	0	0	1	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
1	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0
0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0
1	0	1	1	0	0	0	0	0	1	0	1	1	0	0	0	0
1	0	1	0	1	0	0	0	1	1	0	1	0	1	0	0	1

Figure 1 Encoding

Data Hiding in Audio Signal: (2009), Poulami Dutta1 etal(2), explained information hiding technique is a novel kind of undisclosed communication skill. The mass at nearby information hiding systems uses multimedia stuff like audio. Embedding secret messages in digital sound is frequently a more hard process. Variety of techniques for embedding information in digital auditory has been well-known. In this paper we will attend the general principles of hiding secret information using audio technology, and an overview of functions and techniques. Audio Steganography: A Survey on Recent Approaches (2012), Masoud Nosrati etal(3), in this study, survey on audio steganography recent researches. Due to it, some basic concepts of audio steganography and HAS including Least Significant Bit (LSB) Coding, Parity Coding, Phase Coding, Spread Spectrum (SS) and Echo data hiding are covered. In follow, a brief introduction and abstract of recent methods for audio steganography is presented. Audio Steganography using RSA and GA Based LSB Algorithm to Enhance Security (2011) Juhi Saurabh1 etal(4), he studied the audio steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is a method that ensures secured data transfer between parties normally in internet community. Here we present a novel approach for resolving the problems related to the substitution technique of audio steganography.

In the first stage of security, we use an improved RSA encryption algorithm (RPrime RSA) to encrypt communication, which is extremely complex to split. In the subsequently stage, the encrypted communication is to be programmed into acoustic data for this we use a more commanding GA (Genetic Algorithm) based smallest amount Significant Bit) Algorithm. In order to boost the strength adjacent to planned attacks in which the hackers for all time try to disclose the secreted communication as well as a number of unintentional attacks such as noise adding up, the encrypted communication bits are rooted into chance LSB layers. Here in sequence to decrease distortion, GA operators are used. The essential plan following this manuscript is maintained chance in communication bit placing keen on acoustic facts for hiding the information from hackers and to give a good, well-organized technique for hiding the information from hackers and sent to the reason in a safer way. Reversible information hiding in Encrypted similes by Reserving space previous to Encryption, (2013) Kede Ma etal(5) he explained the more and more attention was paid to reversible data hiding (RDH) in encrypted images, since it maintains the brilliant belongings that the innovative cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. All previous method embeds information by reversibly vacating room from the encrypted images, which may be theme to a quantity of errors on data taking out and/or image restoration. In this paper, we suggest a novel method by reserving room before encryption with a conventional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. The projected technique can attain real reversibility, that is, data extraction and image recovery are free of any error(9). Experiments show that this narrative method can embed more than 10 times as large payloads for the same image quality as the earlier methods, such as for PSNR.

II. Problem Statement And Architecture

A more demanding problem is to secrete data in a two-color double picture (e.g., black-and-white images, such as facsimiles and bar codes). The cause is that altering a pixel can be detected without difficulty. It has significantly low strength adjacent to attacks. (6)For example, if image file entrenched with a top secret communication using LSB coding is resample; the embedded information would be misplaced. This plan ensures that occupied revival of secret information and acoustic using parity method in audio encryption(7). The block diagram of encryption & embedding and extraction and decryption are shown in figure 2 and figure3.

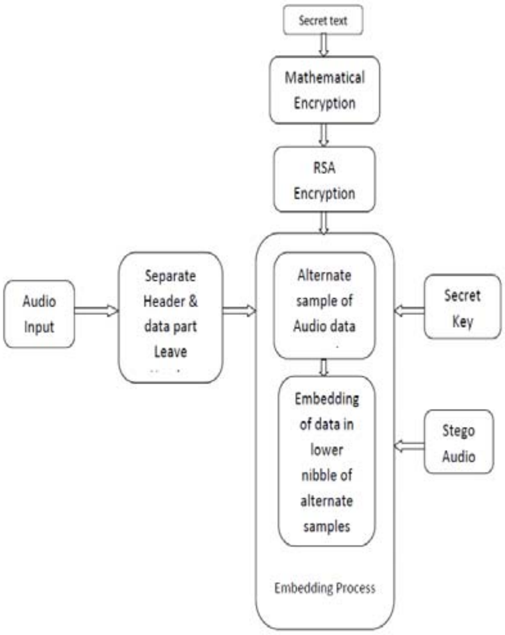

Secret text
Mathematical Encryption
RSA Encryption
Audio Input
Separate Header & data part Leave
Alternate sample of Audio data
Secret Key
Embedding of data in lower nibble of alternate samples
Stego Audio
Embedding Process

Fig 2 Block Diagram of Encryption & Embedding

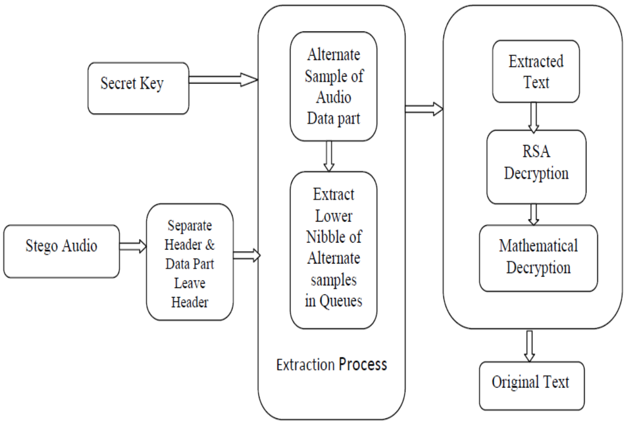

Secret Key
Stego Audio
Separate Header & Data Part Leave Header
Alternate Sample of Audio Data part
Extract Lower Nibble of Alternate samples in Queues
Extraction Process
Extracted Text
RSA Decryption
Mathematical Decryption
Original Text

Fig 3 Block Diagram of Extraction & Decryption

III. Implementation Proposal And Gantt Chart System Specification

HARDWARE REQUIREMENTS

RAM	:	1 GB and above
Processor	:	dual core and above
Hard Disk	:	80 GB and above

SOFTWARE REQUIREMENTS

Operating System	:	Windows XP
Language	:	C#.NET
Software Tool	:	Visual Studio 2010
GUI	:	Windows Application
Database	:	SQL Server (SQL 2008)

GANTT CHART

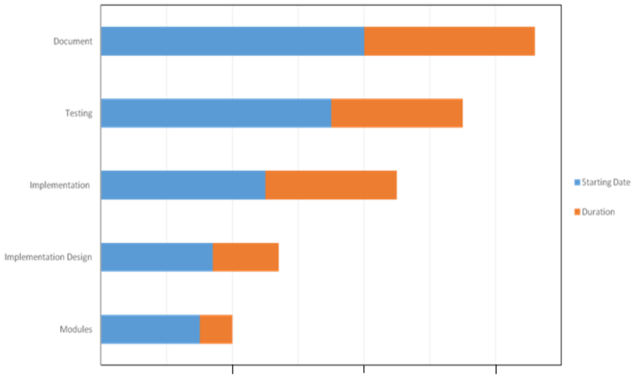


Fig 4 Gantt chart

Steganography is a powerful instrument which increases security in data transferring and archiving. In the steganography scenario the change data is first hidden within one more object which is called “cover object”, to form “stego object” and then this new object can be transmitted or saved. It causes the existence of the convert data and even their transmissions become hidden(17). Steganography is often puzzled with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output(8); the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganalysis is process to detect of presence of steganography. A steganographic method of embedding textual information in an audio file is presented in this paper.(9) In this paper, first the audio file is sampled and then an appropriate bit of each alternate sample is altered to embed the textual information. ETAS model - Embedding Text in Audio Signal that embeds the text like the existing system but with encryption that gains the full advantages of cryptography. In this method for digital audio steganography where data is encrypted using (Rivert SHA) algorithm and embedded into the host audio signal using parity technique(10). Today‟‟s large demand of internet applications requires data to be transmitted in a secure manner , so audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. For a digital data hiding system to be effective and practical, it should exhibit the following characteristics(11).

1) Imperceptibility:
Embedding this extra data must not degrade human perception about the object. Namely, the convert data should be „„„inaudible‟‟‟‟ in stego digital music. Evaluation of imperceptibility is usually based on an objective measure of quality, called signal-to-noise ratio (SNR), or a subjective test with specified procedures.(12)

2) Security:
The data hiding procedure should rely on secret keys, not the algorithm’s secrecy, to ensure security, so that pirates cannot detect or remove secure data by statistical analysis from a set of audio signals. The algorithm should be published and an unauthorized user, who may even know the exact data hiding algorithm, cannot detect the presence of hidden data,(13)unless he/she has access to the secret keys that control this data-embedding procedure.

3) Data Payload:
The data payload refers to the number of bits that are embedded into original audio within a unit of time. It is measured by bps (bit per second). The objective of a steganographic algorithm is to increase payload as much as possible.

4) Real-time processing:
Convert data should be rapidly embedded into the host signals without much delay, so that integrated streaming/data hiding functionality in the delivery of audio over a network can be enabled. Also, a web crawler should support fast data extraction/detection(15).

This data hiding using parity in audio signal consist the following module.

1. Parity Coding.
2. Audio Encryption.
3. Data Hiding in Encrypted Audio.
4. Data Extraction and Audio Recovery.

1. Parity Coding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice Information Hiding in Image and Audio Files in encoding the secret bit.

2. Audio Encryption

In the audio encryption first self reversible embedding the audio .After rearranged self-embedded audio, denoted by **X** , is generated, we can encrypts to construct the encrypted audio, denoted by **X** .With a stream cipher, the encryption version of **X** is easily obtained. such that

$$\mathbf{X}_{i,j}(k) = \left\lfloor \frac{\mathbf{X}_{i,j}}{2^k} \right\rfloor \bmod 2, \quad k = 0, 1, \ldots, 7.$$

3. Data Hiding in Encrypted audio

Once the data hider acquires the encrypted image **E**, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of **A**, denoted by $\mathbf{A}_E$. Data hide by data hiding key.

4. Data Extraction and Image Recovery

Both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a dissimilar condition that the user requirements to take out the audio signals first by audio encryption key or customer desire to extract data first by data encryption key when it is desirable.RSA is the most extensively used public key algorithm.It is named after its creators-Rivest,Shamir and Adleman(14).RSA standard is simple that it is easy to multiply two prime numbers but it is very difficult to factor the product and get them back. RSA Algorithm is as follows:-

1. Take two very large prime no. A & B of equal length and obtain their product (N)
   N = A*B
2. Subtract 1 from A as well as B and take product (T)
   T = (A-1) (B-1)
3. Choose the public key (E) which is a randomly chosen no. such that it has no common factor with T.
4. Obtain the private key(D) as follows
   The rule for encryption of a block of message M into cipher text(C) is as follows:
   C=mod N
6. Message M is raised to power of E (public key) & then divided by N. Remainder of this division is sent as cipher text C.
7. Received message C at the receiver is decrypted as follows:
   M =mod N

In proposed model, the message is first encrypted and then embedded in the carrier. Embedding of encrypted data is done in every alternate bytes lower nibble of audio carrier(16).

The system has following four steps:
1. Encryption
2. Embedding
3. Extraction
4. Decryption

1. Encryption:
First Mathematical encryption and then RSA encryption algorithm is used to enhance the security further.

2. Embedding:
The process of hiding the message in the audio file. Lower nibble of each alternate sample of audio file is embedded by encrypted message bits.
In encryption part mathematical and RSA encryption method is used. In embedding part lower nibble of each alternate sample of data part is embedded. Fig 2.Block Diagram of Encryption & Embedding

3. Extraction:
Is a process of retrieving the message from the lower nibble bits of alternate sample of audio file are taken in one queue.

4. Decryption:
Decryption is simply the inverse of encryption, RSA decryption and arithmetical decryption done on extracted bits in queue.
The screen .shots for the steps are shown in the below figures 5-9.

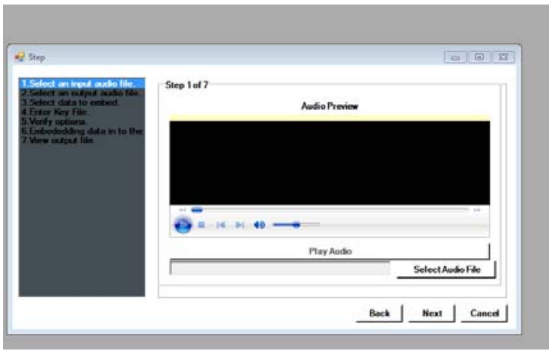


Figure 5 Selecting Audio File

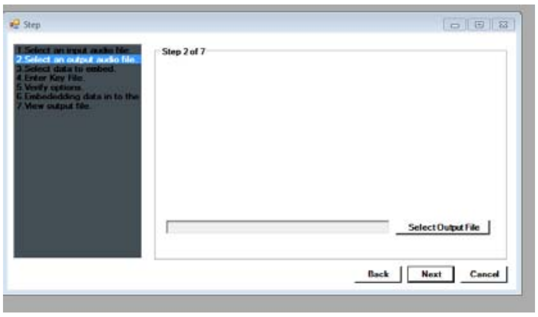
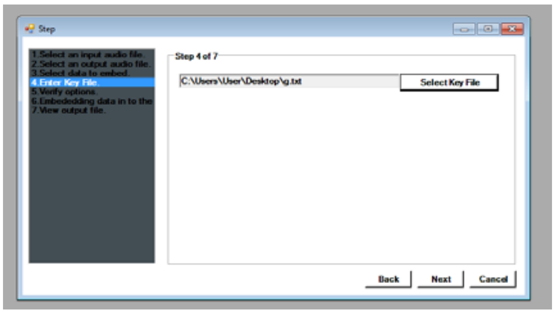
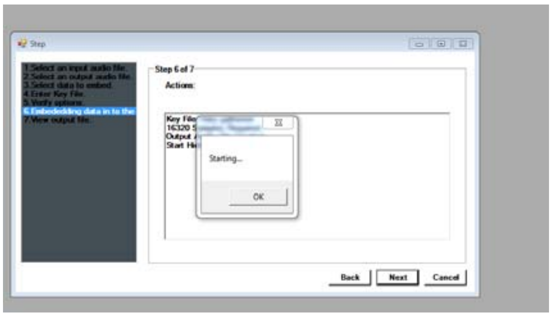


Figure 6 Select output audio file



C:\Users\User\Desktop\g.txt

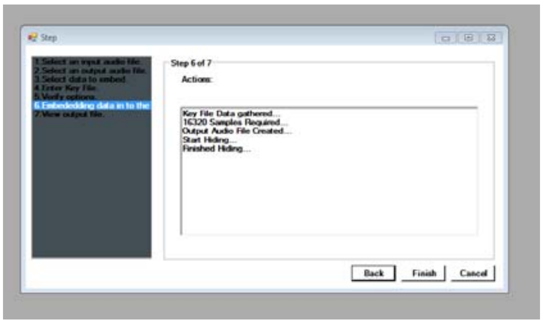
Figure 7 Enter key



Key File
16320 S
Output A
Start Hi

Starting...

Figure 8 verifying key



Key File Data gathered...
16320 Samples Required...
Output Audio File Created...
Start Hiding...
Finished Hiding...

Figure 9 Embedding data

IV. CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Audio file Steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at Steganography to circumvent such policies and pass messages covertly. Although the algorithm presented is a simple one and not without its drawbacks, it represents a significant improvement over simplistic steganographic algorithms that do not use keys. By using this algorithm, two parties can be communicated with a fairly high level of confidence about the communication not being detected. In designing the "Steganography" utmost care was taken to meet user requirements as much as possible. The analysis and design phase was reviewed. Care was taken strictly to follow the software engineering concepts and principles so as to maintain good quality in the developed system as per the user requirements.

Thus by the use of this technique will increase the data security transmission with the audio data. This will useful for the data transmission by the top secret areas like defense etc.

REFERENCES

1. Mohammed Salem Atoum, Osamah Abdulgader Al- Rababah , Alaa Ismat Al-Attili, New Technique for Hiding Data in Audio File IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, April (2011).
2. Data Hiding in Audio Signal: A Review International Journal of Database Theory and Application, Poulami Dutta1, Debnath Bhattacharyya1 and Tai-hoon Kim Vol. 2, No. 2, June (2009)
3. Audio Steganography: A Survey on Recent Approaches World Applied Programming, Masoud Nosrati, Ronak Karimi, Mehdi Hariri, Vol (2), No (3), March (2012)
4. Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security International Journal of Science and Research (IJSR) Juhi Saurabh1, Asha Ambhaikar Audio Steganography, 2011.
5. Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption IEEE Transactions on information forensics and security, Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li, vol. 8, no. 3, march 2013.
6. Basu, P. N.; Bhowmik T., "On Embedding of Text in Audio– A case of Steganography", International Conference on Recent Trends in Information, Telecommunication and Computing, 2010.
7. Poulami Dutta, Debnath Bhattacharyya and Tai-hoon Kim,"Data Hiding in Audio Signal: A Review",International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.
8. Zameer Fatima and Tarun Khanna , "Audio Steganography Using DES Algorithm", Proceedings of the 5th National Conference: Computing For Nation Development, March 10 – 11, 2011 Bharati Vidyapeeth"s Institute of Computer Applications and Management, New Delhi ISSN 0973-7529 ISBN 978-93-80544-00-7.
9. K.P.Adhiya & Swati A. Patil, -"Hiding Text in Audio Using LSB Based Steganography", Information and Knowledge Management www.iiste.orgISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 2, No.3, 2012.
10. Jayaram, Ranganatha, Anupama, -"Information Hiding Using Audio Steganography – A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.
11. Bandyopadhay S. K.; Datta B.; Dutta K., "Information Hiding in Higher LSB Layer in an Audio Image", International Journal of Advanced Research in Computer Science, Vol. 2, No. 3, 2011.
12. William Stalings,"Cryptography and Network Security", Prentice Hall of India Private Limited, New Delhi.
13. K.Sakthisudhan, P.Prabhu and P.Thangaraj"Secure Audio Steganography for Hiding SecretInformation"ICON3C 2012,Proceedings published in International Journal of Computer Applications® (IJCA).
14. Samir Kumar Bandyopadhyay and Biswajita Datta "Higher LSB Layer Based Audio Steganography Technique" IJECT Vol. 2, Issue 4, OCT. - DEC. 2011 ISSN: 2230-7109 (Online) | ISSN: 2230-9543.
15. Swati Malviya, Manish Saxena and Dr. Anubhuti Khare "Audio Steganography by Different Methods", International Journal of Emerging Technology and Advanced Engineering , www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012).
16. Robert Krenn, " Steganography and Steganalysis ," An article, January 2004. http://www.krenn.nl/univ/cry/steg/article.pdf
17. http://en.wikipedia.org/wiki/Steganography.