Secure Data Transfer Through a Combination of Steganographic and Cryptographic Encryption Technique

Swasti Saxena

International Research Journal
p-ISSN 2202-2821 e-ISSN 1839-6518 (Australian ISSN Agency)
Vol. 4 No. 2 2014
82800402201402

Secure Data Transfer through a Combination of Steganographic and Cryptographic Encryption Technique

Swasti Saxena

International Research Journal
p-ISSN 2202-2821 e-ISSN 1839-6518 (Australian ISSN Agency)
Vol. 4 No. 2 2014
828004022014 02

Secure Data Transfer through a Combination of Steganographic and Cryptographic Encryption Technique

ABSTRACT – *Security for information has become a great concern in today's internet era. Thus sending sensitive information from one end to another end via common communicating channel has become inevitable. Steganography has various useful applications and the technique employed depends on the requirements of the application to be designed for. For instance, applications may require absolute invisibility of the secret data, larger secret data to be hidden or high degree of robustness of the carrier. This paper aims at studying popular encryption techniques and their drawbacks due to which they could not be put to practical use along with a proposed method of successfully encrypting information both in image and text format combing their successful delivery to the destination using steganographic and cryptographic techniques of information encryption.*

KEY WORDS: STEGANOGRAPHY, SECURITY, ENCRYPTION, WATERMARK, AUTOMATIC REPEAT REQUEST

INTRODUCTION

Human eye is relatively insensitive to high spatial frequencies. Many steganographic algorithms have potentially utilized these facts thus modifying the least significant bits of gray level in digital images or digital sound tracks. The insensitivity of human eye is also figured in its incapability to perceive gradual changes in brightness. By gradual changes over the image by overlaying an irregular pattern, the image becomes more robust with respect to common image processing as embedded information is incorporated into low frequencies. It is important to correctly distinguish between Invisibility, detectability and robustness with respect to intentional and unintentional modifications, and the security.

Steganography is a word with its Greek origin roots. It literally means concealed writing or writing in hiding. Cryptography is different from steganography. In cryptography the message's content is protected while steganography deals with the concealing the very existence of the message. Generally the data is hided in the following way. The embedded data or the secret message which one wishes to send is hidden in an innocuous

message referred to as a cover-text or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object.

By definition, steganographic methods should not visibly modify the carrier. On the same hand the modifications should be unperceivable to human visual system. Data hiding technique can be put to use for various purposes and different requirements and limitations on the appropriate steganographic methods are unique to specific applications. This paper aims at studying popular encryption techniques and their drawbacks due to which they could not be put to practical use along with a proposed method of successfully encrypting information both in image and text format combing their successful delivery to the destination using steganographic and cryptographic techniques of information encryption.

APPLICATIONS OF STEGANOGRAPHY

The field of steganography is very promising and can be put to use for wide variety of applications such as in medical imaging where patient's details are embedded within image providing protection of information and reducing transmission time and cost, for safe circulation of secret data, which is a prime requirement in defense organizations like or in online voting system so as to make elections secure and robust against a variety of fraudent behaviors etc.

POPULAR ENCRYPTION TECHNIQUES AND THEIR DRAWBACKS DUE TO WHICH THEY COULD NOT BE PUT TO PRACTICAL USE

1. Aura [1] proposed the following steganographic method possessing absolute secrecy. To embed a small message of the order of 8 bits or so, just keep scanning an image till a certain password-dependent message digest hash function returns the required 8-tuple of bits. This method has the advantage of absolute secrecy tantamount to one time pad used in cryptography. It guarantees the same error distribution and un-detectability.

DRAWBACKS

Although the scheme satisfies the requirements of a steganographic holy grail, it is time consuming, has very limited capacity, and is not applicable to image carriers for which we only have one copy.

Aura also suggest to play it safe and change only a small fraction of the carrier bits. For example, modify each hundredth pixel in the carrier by one gray level.

Depending on the image noise, these changes will hopefully be compatible with the uncertainties involved with any statistical model of the image.

DRAWBACKS

This technique imposes limits on the maximal capacity of the carrier image, and it can leave traces in the carrier image.

2. Spatial Domain-Based Steganographic Techniques

The simple way to represent pixel's color is by giving an ordered triplet of numbers: red (R), green (G), and blue (B)that comprises particular color. The other way is to use a table known as palette to store the triplet, and put a reference into the table for each pixel. The spatial domain-based steganographic techniques use LSB algorithm for embedding/extraction of data as. In Spatial domain, cover-image is first decomposed into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits. Advantages are high embedding capacity, ease of implementation and imperceptibility of hidden data.

DRAWBACK

The major drawback is its vulnerability to various simple statistical analysis methods.

Frequency domain embedding techniques, which first transforms the cover-image into its frequency domain, secret data is then embedded in frequency coefficients. Advantages include higher level of robustness against simple statistical analysis.

DRAWBACK

Unfortunately, it lacks high embedding.

Fridrich7 proposed a palette modification scheme for hiding data. In this method, both the cost of removing an entry color in a palette and the benefit of generating a new one to replace it are calculated. If the maximal benefit exceeds the minimal cost, entry color is replaced. His method remarkably reduces the distortion of the carrier images.

DRAWBACK

This method suffers with the low embedding capacity.

Table 1: Secret Message Hiding

	Description
PURPOSE	To send a secret message without raising any suspicion that a secret message is being sent.
REQUIREMENT	Secrecy, difficult to detect, large capacity.
REMARKS	Always assume Kerckhoffs principle (protect the embedded Information by a message and carrier independent key), maximize the capacity, minimize key size.

Table 2: Watermarks

	Description
PURPOSE	Copyright protection, proof of ownership, fingerprinting (tracing distributed multiple copies), image integrity protection.
REQUIREMENT	Robustness, difficult to remove even under collusion and Kerckhoffs principle.
REMARKS	We do not require that the watermark not be detectable in the sense of maximum secrecy as in the case of covert communication

Four primary objectives of this research are as follows:

1. Scheming out a method for concealing messages in images by slightly modifying the pixel values in an existing image (a carrier) so that a message or simply a different image can be hidden in the carrier.
2. Extending the schemes to images in graphic formats, which utilize lossy compression algorithms. Since a robustness with respect to small amount of noise and / or to loss of information due to lossy compression is necessary, we intend to work in the Fourier /wavelet space instead of the pixel space.
3. Studying the security, efficiency, and robustness of schemes for hiding messages and implementing the algorithms. The security with respect to known attacks will be investigated.
4. Demonstrating the performance of the hiding schemes on real imagery.

OUR PROPOSED TECHNIQUES

High degree of robustness is required with respect to image modifications including noise and lossy compression, and are extremely secure.

TECHNIQUE 1:

A key dependent image is overlaid by the carrier image whose power is concentrated in the low frequencies. The extraction of the hidden message is based on a discrete cosine transform.

TECNIQUE 2:

The second technique inserts bits of secret messages into projections of image blocks onto random, smooth, orthogonal patterns individually generated for each image and user ID. This way, we avoid using publicly known basis functions, such as discrete cosines, which increases security against malicious attacks.

SECURITY OF OUR TECHNIQUES

By modifying the least significant bit the security can be significantly increased if the consecutive bits of the secret message can be embedded into a pseudo-randomly chosen sequence of pixels of the cover image. While it is certainly possible to design schemes using pseudo-random generators, we propose a scheme in which chaotic permutations [12] are used to randomly scramble the cover image. The secret message consisting of k bits is embedded into the first k pixels of the scrambled image. The inverse chaotic permutation is applied to get the modified cover image. This scheme has the advantage that it is very easily implemented, it is fast, and provides a good security.

Chaotic permutations generated using two-dimensional chaotic maps, such as the baker map [12], depend on a sequence of integers which add up to N - the number of pixels in one row of the cover image. The per\mutations are therefore parameterized by the sequence of integers, which play the role of a secret key without which the retrieval of the message becomes impossible.

The scheme is explained in figure 1.

PROPOSED WAYS FOR PREVENTING ATTACK ON THE ENCRYPTED DATA

There are at least three ways to prevent the attack :

1. One possibility is to use adaptive watermarks whose strength is locally adjusted according to the masking properties of the human visual system.

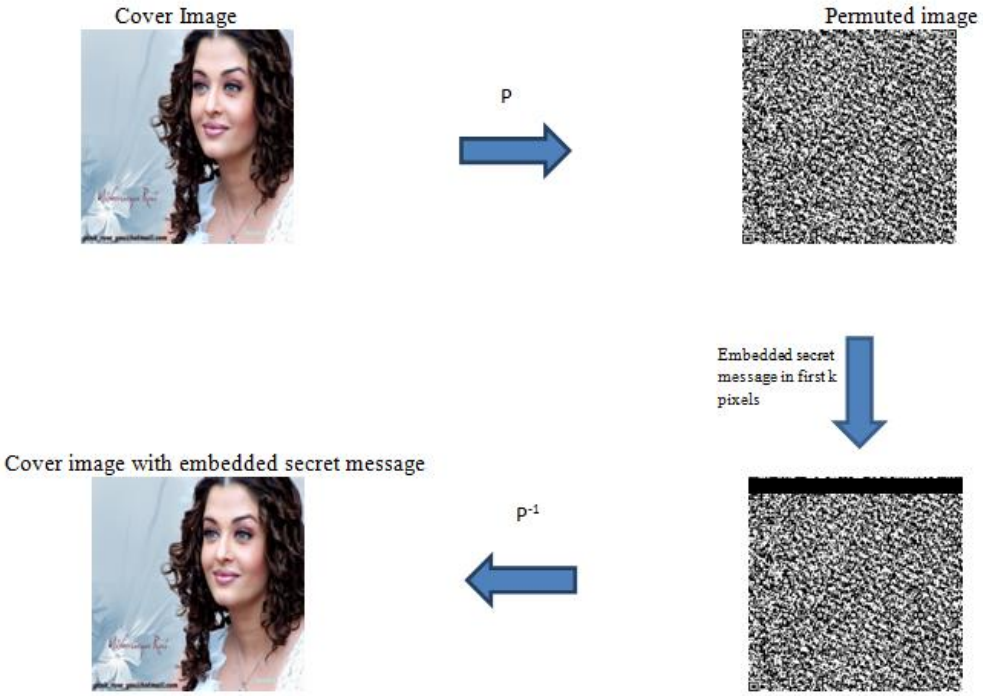

Figure 1: Cover Image Permuted Image

2. The second possibility is to replace discrete cosines with other, key-dependent bases. If the basis functions are not known, this type of attack would not be possible. In order to make this practical, however, we would have to design orthogonal bases which would depend on parameters - a secret key. Another important requirement is that there should exist efficient computational algorithms similar to fast Fourier type of transforms.

3. The third option is to view the watermarking scheme as pattern overlaying. We do not have to use patterns formed by a linear combination of discrete cosines but we could utilize general key-dependent patterns with their power concentrated mostly into low frequencies in order to guarantee robustness. This approach is further elaborated below. To prevent data detection DWT (Discrete Wavelet transform) is used.

METHOD FOR TEXT CONTEXT ENCRYPTION

This method suggests noise filtering in the beginning before embedding. After extraction at receiving end, ARQ (Automatic Repeat Request) is used for error detection &

correction. For secure transmission of data, encryption & data hiding are combined in a single step. Host image and secret data are converted into bit stream. Before encryption of secret data median filtering is used. The input values are converted to ASCII and then to binary, the host image RGB values are converted to binary. Substitution is performed character by character using encryption key. The LSB of every pixel octet is replaced by secret bit stream. Error detection and correction ensures correct transmission of data.

REFERENCES

[1]. Nirinjan, U.C. & Anand, D. "WATERMARKING MEDICAL IMAGES WITH PATIENT INFORMATION". In the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 1998, pp. 703-06.

[2]. Katiyar, S.; Meka, K.R.; Barbhuiya, F.A. & Nandi, S. "ONLINE VOTING SYSTEM POWERED BY BIOMETRIC SECURITY USING STEGANOGRAPHY". 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, India, 2011, pp. 288-291.

[3]. Jaswinder Kaur, Inderjeet & Manoj Duhan, "A COMPARATIVE ANALYSIS OF STEGANOGRAPHIC TECHNIQUES", IJITKM, Vol.2, No. 1 2009.

[4]. Hao-Tian Wu and Jean-Luc Dugelay , (2009) "STEGANOGRAPHY IN 3D GEOMETRICS AND IMAGES BY ADJACENT BIT MAPPING", EURASIP Journal on Information Security, Vol. 2009, Article ID 317165, pp1-10. IJCSES Vol.4, No.6, December 2013

[5]. Brassil J., S. Low, N. Maxemchuk, L. O'Goram, "HIDING INFORMATION IN DOCUMENT IMAGES," CISS95. ftp://ftp.research.att.com/dist/brassil/1995/ciss95.ps.Z

[6]. Comiskey, B. O. and J.R. Smith, "MODULATION AND INFORMATION HIDING IN IMAGES," in: Information Hiding, First International Workshop, edited by Ross J. Anderson. Cambridge, U.K., May 30-June 1, 1996, Proceedings. Lecture Notes in Computer Science, Vol. 1174, Springer-Verlag, 1996 http://sunsite.informatik.rwth-aachen.de/dblp/db/conf/ih/ih96.html

[7]. Cox, J. L, J. Kilian, T. Leighton, and T. Shamoon, "SECURE SPREAD SPECTRUMWATERMARKING FOR MULTIMEDIA," NEC Research Institute, Technical Report 95-10.

[8]. Craver, S., N. Memon, B.-L. Yeo, and M. Yeung. "CAN INVISIBLE WATERMARKS RESOLVE RIGHTFUL OWNERSHIPS?" Proceedings of the IS&T/SPIE Conference on Storage and Retrieval for Image and Video Databases V, San Jose, CA, USA, Feb. 13-14, 1997, vol. 3022, pp. 310-321.

[9]. Delaigle, J.-F., C. De Vleeschouwer, B. Macq, "DIGITAL WATERMARKING OF IMAGES," Proceedings of the IS&T/SPIE Symposium on Electronic Imaging Science and Technology,1996.

[10]. Dixon R. C, SPREAD SPECTRUM SYSTEMS WITH COMMERCIAL APPLICATIONS. Wiley, New York, 1994.

[11]. Fridrich, J., "ON DIGITAL WATERMARKS," paper for the 2nd Information Hiding Workshop in Portland, Oregon, April 15-17, 1998.

[12]. Fridrich, J. "SYMMETRIC CIPHERS BASED ON TWO-DIMENSIONAL CHAOTIC MAPS," to appear in Int. J. Bifurcation and Chaos, 8(6), June 1998.

[13]. Girod B. and F. Härtung, "WATERMARKING METHOD AND APPARATUS FOR COMPRESSED DIGITAL VIDEO", US Patent application, 1996. http://www-nt.e-technik.unierlangen. de/~hartung/watermarking.html

[14]. Handel and Sanford http://www.lanl.gov/users/u078743/embedl.htm

[15]. Maxwell T. Sandford U, Jonathan N. Bradley, and Theodore G. Handel. "THE DATA EMBEDDING METHOD". In Proc. of the SPIE Photonics East Conference, Philadelphia, September 1995.

[16]. Härtung F. and B. Girod, "DIGITAL WATERMARKING OF RAW AND COMPRESSED VIDEO", Proc. European EOS/SPIE Symposium on Advanced Imaging and Network Technologies, Berlin, Germany, Oct. 1996.

– END –