Text Security Using PNG

Shital B. Deshmukh[1], Prof.Vikas P. Mapari[2]
[1]Dept of Computer
[2]Asst. Professor, Dept of Computer
[1, 2] D.Y.Patil,C.O.E.,Ambi,Pune, India

Abstract- *Data is an important asset for any individual or organization and must be protected from intruders or hackers. The need to hide data from hackers has existed since ancient times, and nowadays, there are developments in digital media, such as audio, video, images, and so on. To secure secret information, different media methods are used and steganography is one. Steganography hides the data under other data without any differentiable changes. Many individual steganography tools can be used to transfer data securely and, in this report, a new tool is proposed that decreases time and effort. Using this tool, we hide the text in images in one place, so there was no need to have access to multiple tools. This proposed tool developed using the least significant bit (LSB) approach.*

Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. There for from time to time researchers have developed many techniques to fulfil secure transfer of data and steganography is one of them. In this paper we have proposed a new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form.

Keywords- Cryptography, Steganography, LSB, Hash LSB, RSA Encryption, Decryption.

I. INTRODUCTION

Globalization has led to the rapid growth of the internet through which consumers can send and receive large amounts of data (e.g., text, audio and images). In modern communication systems, securing data is of utmost importance. Yet sending and receiving secret files over the internet is still insecure, and therefore hiding data in an effective way protects this secret information. Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference.

Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the

Protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data.

Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction.

II. REVIEW OF LITERATURE

K. Hwang and D. Li, Trusted cloud computing with secure resources and data coloring, IEEE Internet Comput., vol. 14, no. 5, pp. 1422.2014

Cloud computing enables a new business model that supports on-demand, pay-for-use, and economies-of-scale IT services over the Internet. The Internet cloud works as a service factory built around virtualized data centers.1 Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a service-oriented platform using virtual server clusters at data centers. However, a lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing

services. To promote multitenancy, we must design the cloud ecosystem to be secure, trustworthy, and dependable. 5 In reality, trust is a social problem, not a purely technical issue. However, we believe that technology can enhance trust, justice, reputation, credibility, and assurance in Internet applications. To increase the adoption of Web and cloud services, cloud service providers (CSPs) must first establish trust and security to alleviate the worries of a largenumber of users. A healthy cloud ecosystem should be free from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations. Both public and private clouds demand trusted zones for data, virtual machines (VMs), and user identity, as VMware and EMC3 originally introduced.

F. Bao, R. H. Deng, B. C. Ooi, and Y. Yang, Tailored reversible watermarking schemes for authentication of electronic clinical atlas, IEEE Trans. Inf. Technol. Biomed., vol. 9, no. 4, pp. 554563, Dec. 2016.

Efficient maintenance of medical data in an electronic format is crucial for enhancing the quality and efficacy of healthcare through efficient information sharing. However, along with the benefits is the growing concern about the security of digital medical information. In a broad sense, security issues pertaining to digital medical data are categorized into the following aspects: 1) Confidentiality: individual privacy of patients as well as physicians implies that medical data must be protected from inappropriate disclosure. Only authorized users with appropriate rights are offered access to the data. 2) Authentication: authentication (reliability in [1] and [2]) of medical data can be further classified into a) integrity: medical information must be assured of its intactness; b) authenticity: credibility must be given to the users that the underlying data are what they are claimed to be. 3) Availability:medical datamust be guaranteed to be readilyavailable to the authorized users. Medical imaging constitutes an important part of digitalmedical data. Clearly, the attacks that threaten digital medical information as a whole (see e.g., [3] and [4]) would also apply to medical images. In this paper, we explor the authentication aspect of medical images. Multimedia authentication inherits many characteristics of generic data authentication using cryptographic primitives, such as integrity verification, authenticity verification, and nonrepudiation [5]. However, multimedia authentication has its own unique features that make the techniques for generic data authentication insufficent and sometimes undesirable. For example, an image changing from one format to another without losing visual content should be deemed authentic in multimedia authentication, whereas this turns out to be hard to achieve by applying generic data authentication that uses message authentication code (MAC) or digital signature [5]. As a result, multimedia authentication is normally accomplished by digital watermarking [6], [7]. Digital watermarking can be classified into copyright watermarking and authentication watermarking, based on the purposes it is intended for. We note watermarking can also be used to establish a channel for carrying, e.g., meta-data [8][10]. In a strict sense, this application of watermarking belongs to the area of steganography, since the objective is to hide medical data in a host image for data secrecy purposes.

In copyright, the inserted 6 mark, upon extraction, asserts ownership of the underlying data. To achieve this end, copyright watermarkingmust be robust so that the inserted mark cannot be easily removed. In contrast, authentication watermarking is designed to prove the integrity and authenticity of the underlying data. Authentication watermarking can be further classified into hard authentication and soft authentication Watermarking working in such a reversible way is referred to as reversible (lossless, invertible, distortion free, erasable, etc.) watermarking [13][18] in the literature. Reversible watermarking is regarded as a special form of hard authentication [11]. In this paper, we develop reversible watermarking schemes that are tailored for authentication of the electronic clinical atlas [19][21], a particular type of medical images in palette format.

V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, Reversible watermarking algorithm using sorting and prediction, IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989999, Jul. 2015.

Lossless data hiding techniques hide data in a host signal (for example, an image) and allow extraction of the original host signal and also the embedded message. There are two important requirements for reversible data hiding techniques: the embedding capacity should be large; and distortion should be low. These two requirements conflict with each other. In general, a higher embedding capacity results in a higher degree of distortion. An improved technique embeds the same capacity with lower distortion or vice versa. Tians difference expansion technique [15] previously had the highest embedding capacity and the lowest distortion in image quality. His method divides the image into pairs of pixels and uses each legitimate pair for hiding one bit of information. Therefore, his embedding capacity is at best 0.5 b/pixel. However, an uncompressed location map also needs 0.5 b/pixel. Then, it is 7 impossible to hide data reversibly into an image. Thus, reducing the size of the location map is one of the key goals in this field.

Without a location map, the decoder cannot decode exactly because it does not know howand which cells were modified. The location map consists of flags, which are either 0 or 1. The purpose of the flags differs between the particular methods. The difference expansion technique is the seminal reversible data hiding scheme andwas the basis for new ideas, such as Alattars technique for triplets and quads [1], [2], and Kamstra and Heijmans sorting method [7]. Alattar has expanded one cell from a pair to a triplet [1] or quad [2] to hide two or three bits per cell, respectively, or none at all in illegitimate cells. A cell is the unit of pixels in which the data is to be embedded.

AL attars location map covers all triplets or quads instead of pairs. Thus, the uncompressed location map size is decreased from one-half of the image resolution (for Tians method) to one-third or one-fourth of the resolution (for triplets or quads), respectively. It is obvious that Alattars methods have advantages over Tians, since the forms can hide data even if the location map is not compressed whereas it is not possible in Tians method. If the location map is compressed, Alattars method significantly outperforms Tians method. Later Alattar generalized his idea for a cell with n pixels in [3].

W. Zhang, X.Hu, X. Li, and N. Yu, Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression, IEEE Trans. Image Process., vol. 22, no. 7, pp. 27752785, Jul. 2016

As a technique that embeds the secret message into cover signals, information hiding has been widely applied in areas such as covert communication, media annotation and integrity authentication. Reversible data hiding (RDH) is one kind of information hiding techniques with the characteristics such that not only the secret message needs to be precisely extracted, but also the cover itself should be restored losslessly. This property is important in some special scenarios such as medical imagery [1], military imagery and law forensics. The sorting technique
[11] and pixel selection

- give priority to prediction errors in smooth regions, so a sharper histogram can be obtained. After generating a good histogram for RDH, the following two problems are: 1) what is the maximum embedding rate for the given histogram and distortion constraint; 2) how to realize the optimal modification on the histogram for achieving the maximum embedding rate? Herein, embedding rate is defined as the average number of message bits carried by one host signal.

B.ou, X. Li, Y. Zhao, R. Ni, and Y. Shi, Pairwise prediction-error expansion for efficient reversible data hiding, IEEE Trans. Image Process., vol. 22, no. 12, pp. 50105021, Dec. 2013.

Data hiding offers a way to embed data into cover medium for the purposes of ownership protection, authentication, fingerprinting, secret communication and annotation [1][3], etc. In most data hiding algorithms, the cover data is destroyed permanently and cannot be exactly restored after the embedded message is extracted. Recently, a new data hiding technique, namely, reversible data hiding (RDH) [4][6], is proposed, in which both the cover data and the embedded message can be extracted from the marked content. This specific data hiding technique has been found to be useful in the military, medical and legal fields, where the recovery of the original content is required after data extraction. Novel RDH framework based on the so-called pairwise PEE is proposed. In contrast to the prior PEE methods, we first take every two adjacent prediction-errors as a unit to generate a sequence consisting of prediction-error pairs, then obtain a two-dimensional prediction-error histogram (2D PEH), and finally, embed data by using pairwise PEE, the basic principle of the conventional PEE used for 1D PEH is reviewed.

I.-C. Dragoi and D. Coltuc, Local-prediction-based difference expansion reversible watermarking, IEEE Trans. Image Process., vol. 23, no. 4, pp. 17791790, Apr. 2014.

While classicalwatermarking introduces permanent distortions, reversiblewatermarking not only extracts the embedded data, but also recovers the original host signal/image without any distortion. So far, three major approaches have already been developed for image reversible watermarking. They are reversible watermarking based on lossless compression, on histogram shifting and on difference expansion. The lossless compression based approach substitutes a part of the host with the compressed code of the substituted part and the watermark [1], [2], etc. In order to avoid artifacts, the substitution should be applied on the least significant bits area where the compression ratio is poor. This limits the efficiency of the lossless compression reversible watermarking approach. A more efficient solution is the histogram shifting approach. The histogram of a pixel based image feature (graylevel [3], pixel difference [4], prediction error [5], interpolation error [6]) is considered. A histogram bin is selected and the space for data embedding is created into an 10 adjacent bin (either the bin located at the left or at the right). For instance, let pbe the value of the selected bin and let p+1 (the bin to its right) be considered for data embedding.

The features greaterthan p are shifted with one position (by modifying with one graylevel the value of the corresponding pixels). Furthermore, the embedding is performed into the pixels with the feature value equal to p. When a zero is embedded the pixel is left unchanged, otherwise it is modified with one graylevel in order to change the feature from p to p + 1. Instead of pursuing a single sharp PE histogram, we design the pixel predictors for the sake of minimizing the conditional entropy of the PE sequence by utilizing mixture of Gaussian distributions. And correspondingly, a novel optimized multiple histograms modification scheme is presented to finally embed messages into the generated Gaussian mixture of PE sequence, which automatically allocates different amount of data into different groups of pixels like the schemes in [27]. Actually, for a given PE sequence, the upper bound of the embedding rate under an input distortion constraint is given by (??). So instead of using the expanding and shifting technique described in [11], Lin et al. [16] proposed a pixel by pixel code construction to approach the rate distortion bounds for distortion metrics like square error distortion or L1-Norm distortion. And alternatively, by improving the recursive code construction (RCC), we obtain the optimal embedding method for general gray-scale PE sequences [20], which performs in a bin by bin manner respectively.

J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890896, Aug.2013.

Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload)into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An intriguing feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state. The performance of a reversible data-embedding algorithm can be measured by the following. 1) Payload capacity limit: what is the maximal amount of information can be embedded? 2) Visual quality: how is the visual quality on the embedded image? 3) Complexity: what is the algorithm complexity? The motivation of reversible data embedding is distortion- free data embedding

- Though imperceptible, embedding some data will inevitably change the original content. Even a very 16 slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required. From the application point of view, reversible data embedding can be used as an information carrier. Since the difference between the embedded image and original image is almost imperceptible from human eyes, reversible data embedding could be thought as a covert communication channel.

By embedding its message authentication code, reversible data embedding provides a true self authentication scheme, without the use of metadata. In this paper, we present a high-capacity, high visual quality, reversible data-embedding method for digital images. Our method can be applied to digital audio and video as well. We calculate the differences of neighboring pixe values, and select some difference values for the difference expansion (DE). The original content restoration information, a message authentication code, and additional data (which could be any data, such as date/time information, auxiliary data, etc.) will all be embedded into the difference values. In this paper we will consider grayscale images only. For color images, there are several options. One can decorrelate the dependence among different color components by a reversible color conversion transform [2], and then reversibly embed the data in the decorrelated components. Or one can reversibly embed each color component individually.

III. SYSTEM ARCHITECTURE

3.1 Overview

It is possible to alter graphic or sound files slightly without losing their overall viability for the viewer and listener. With audio, you can use bits of file that contain sound not audible to the human ear. With graphic images, you can remove redundant bits of color from the image and still produce a picture that looks intact to human eye and is difficult to discern from its original. It is in those bits that stego hides its data.

A stego program uses an algorithm, to embed data in an image file, and a password scheme to allow you to retrieve information. Hiding the text message in an image file. Encryption of the same message, so as to support more secure steganography. The decoding of the message, decryption and source message

3.2 Technical Model

It is a science of exchanging the information in a method that hides the existence of exchanging the information. If compared with the cryptography, in the cryptography the enemies are permitted to detect, intercept and change messages without violating certain premises and the target of steganography is to hide the information within other messages that does not permit the enemies to even know that there are secret messages present. The general principle in the steganography is by replacing the high entropy noise with a strong entropy secret transmission.

3.3 Hiding Secret Messages in Digital File

Hiding a secret file in a cover file, we began by selecting a key file and an acceptable cover file. The tool alters and modifies the bits of the cover image to allow the insertion of the secret message in the cover image. After this insertion is completed, a new, acceptable file is generated. This new file is called a stego file.

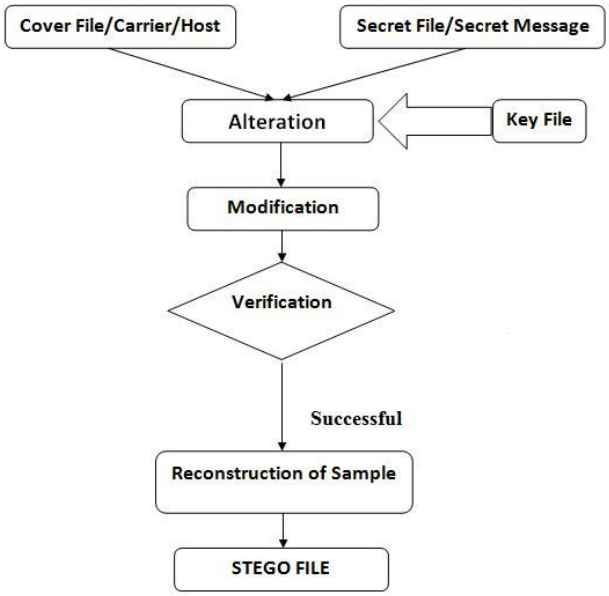

Fig1. Encryption Model

3.4 Secret Message Extraction

the process of extracting the secret message from the stego file. To extract the secret message, we need the same key file we used to hide the message. We begin by verifying that key file. After verification is successful, the tool extracts the secret message from the cover file.

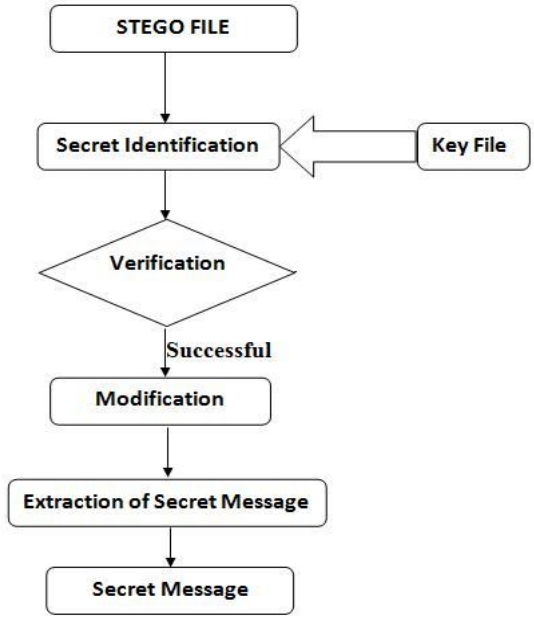

Fig.2 Decryption Model

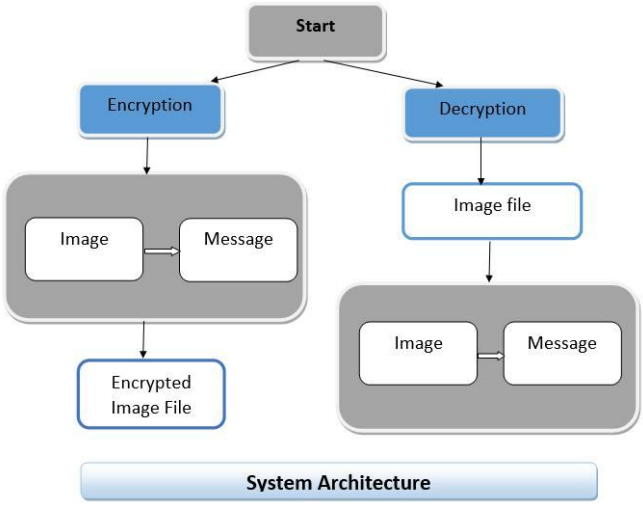

Fig.3 System Architecture

IV. MATHEMATICAL MODEL

Any steganographic algorithm or simply Stego-algorithm is composed of Stego-Function Ғ and inverse of Stego-Function Ғ-1. Ғ takes Cover-Image C and Information I as input and generates Stego-Image S as the output. At the receiver end the Stego-Image S is fed to decoding algorithm which is mathematically inverse of Stego-Function Ғ(represented as Ғ-1) and produces Information I. These two function along with the entire set of their domain and co-domain form the Steganographic System Ψ (or simply Stego-system).

Mathematically this can be represented as S = Ғ(C, I) and

I = Ғ-1

(S) and Ψ = {Ғ, Ғ-1, C, S, I}.

Universal Stego System:

A perfect Depicter of a Stego-Algorithm A same stego-algorithm may operate on different cover images and may insert different information's in them. So any stego system Ψ = {Ғ, Ғ-1, C, S, I} is different for every pair of cover image C and Information I even though the Algorithm of Stego- system Ψ given as Ψ(Algorithm) = { Ғ, Ғ-1} remains the same for all those pairs. So we introduce the concept of Universal Stego

System which is Universal Set of all stego systems Ψ = {Ғ, Ғ-1, C, S, I} which have same Stego-Algorithm Ψ(Algorithm) ={ Ғ, Ғ-1}. We represent any Universal Stego System by Φ ={Ғ, Ғ-1, ℂ , , } where is set of all cover Images, is set of all stego-images and is set of all Information and stego algorithm of Φ given as Φ(Algorithm) = { Ғ, Ғ-1}. Thus any stego system Ψ = {Ғ, Ғ-1, C, S, I} is an instance of or Universal Stego System Φ = {Ғ, Ғ-1, ℂ, , }. Mathematically we represent a Universal Stego System Φ as:

$$\Phi = \{Ғ, Ғ\text{-}1, ℂ, ,\}$$

{x=x is stego system Ψ = {Ғ, Ғ-1, C, S, I} with stego algorithm { Ғ, Ғ-1}

Stego System Φ = {Ғ, Ғ-1, ℂ, , } with stego algorithm { Ғ, Ғ-1}}

Where,

ℂ = {C:C is the set of Cover Images}
= {S: S is the set of Stego Images}
= {I: I is the set of all Information}

Ψ = {Ғ, Ғ-1, C, S, I} and Ψ € Φ

System Description: -

Let the system be described by S,

$$S = \{I,ERP,DRP,K,R\}$$

Where,

I = Input
ERP = Encryption Process
DRP = Decryption Process
K = Secrete Key
R = Result

V. ACKNOWLEDGMENT

When the completion of dissertation report comes to an end, the time comes to acknowledge all persons who have made its success possible. It gives me immense pleasure to express our gratitude to each individual associated directly or indirectly with the successful completion of the this paper.

I would like to take this opportunity to specially thank my guide, Prof. Vikas Mapari, Department of Computer Engineering, D Y Patil College of Engineering, Pune, for vesting trust in me.

I would like to especially thanks to Prof. Dhanshree S. Kulkarni, Head, Department of Computer Engineering, for inspiring me and providing me all the Internet Lab Facility, which made this seminar work convenient.

I would also like to specially thank to Dr. Abhay A. Pawar, Principal, D Y Patil College of Engineering, Pune for all required facilities in our M. E. degree course. My thanks are also to all faculty members of my department.

VI. CONCLUSION

Steganography is useful for hiding messages for transmission. One of the major discoveries of this investigation was that each steganographic implementation carries with it significant trade-off decisions, and it is up to the steganographer to decide which implementation suits him/her best. Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

REFERENCES

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain A New Approach for LSB Based Image Steganography using Secret Key, International

Conference on Computer and Information Technology (ICCIT), Pages No. 286 291, 22-24 Dec., 2011..

[2] Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, Hash Based Least Significant Bit Technique for Video Steganography (HLSB), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[3] Mamta Juneja, Parvinder Singh Sandhu, Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption, International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 305, 27-28 Oct., 2009.

[4] Swati Tiwari, R. P. Mahajan, A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion, International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[5] N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen, IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.

[6] Wien Hong, Tung-Shou Chen, A Novel Data Embedding Method Using Adaptive Pixel Pair Matching, IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.

[7] Amr A. Hanafy, Gouda I. Salama, Yahya Z. Mohasseb, A Secure Covert Communication Model Based on Video Steganography, Military Communications Conference, IEEE, Pages No. 1 6, 16-19 Nov., 2008.

[8] R. Chandramouli, N. Memon, Analysis of LSB based image Steganography techniques, International Conference on Image Processing, Vol. 3, Pages No. 1019 1022, 07 Oct 2001-10 Oct, 2001.

[9] Weiqi Luo, Fangjun Huang, Jiwu Huang, Edge Adaptive Image Steganography Based on LSB Matching Revisited, IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 214, June, 2010.

[10] Ross J. Anderson, Fabien A. P. Petitcolas, On the Limits of Steganography, IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 481, May, 1998.

[11] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, A High Capacity 3D Steganography Algorithm, IEEE Transactions on Visualization and Computer Graphics, Vol. 15, Issue No. 2, Pages No. 274 284, March-April, 2009.

[12] Nicholas Hopper, Luis von Ahn, John Langford, Provably Secure Steganography, IEEE Transactions on Computers, Vol. 58, Issue No. 5, Pages No. 662 676, May,2009.

[13] Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, RGB Intensity Based Variable-Bits Image Steganography, Asia-Pacific Services Computing Conference, IEEE, Pages No. 1322 1327, 9-12 Dec., 2008.

[14] Jing-Ming Guo, Thanh-Nam Le, Secret Communication Using JPEG Double Compression, Signal Processing Letters, IEEE, Vol. 17, Issue No. 10, Pages No. 879 882, Oct., 2010.

[15] Weiqi Luo, Yuangen Wang, Jiwu Huang, Security Analysis on Spatial 1 Steganography for JPEG Decompressed Images, Signal Processing Letters, IEEE, Vol. 18, Issue No. 1, Pages No. 39 42, Jan., 2011.

[16] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, pp. 137–150, 1996.

[17] D. Gruhl, A. Lu, and W. Bender, "Echo hiding," in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, pp. 295–315, 1996.

[18] J. Gurnsey, Copyright Theft. Aslib Gower, 1995.

[19] R. Hart, "A voluntary international numbering system—The latest WIPO proposals," Computer Law and Security Report, vol. 11, no. 3, pp. 127–129, May–June, 1995.

[20] J. N. Holmes, Speech Synthesis and Recognition—Aspects of Information Technology. London, U.K.: Chapman & Hall, 1993.

[21] Talk on software birthmarks, counsel for IBM Corporation, BCS Technology of Software Protection Special Interest Group, London 1985.

[22] G. Jagpal, "Steganography in digital images," Thesis, Cambridge Univ. Comput. Laboratory, Cambridge, Univ. Cambridge, U.K., May 1995.

[23] D. Kahn, The Codebreakers. New York: Macmillan, 1967.

[24] A. Kerckhoffs, "La cryptographie militaire," J. des Sciences Militaires, ser. 9, no. IX, pp. 5–38, Jan. 1883, pp. 161– 191, Feb. 1883.

[25] E. Koch and J. Zhao, "Toward robust and hidden image copyright labeling," in Proc. 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Halkidiki, Greece, June 20–22, 1995.

[26] H. M. Kriz, "Phreaking recognized by directorate general of France telecom," Chaos Digest 1.03, Jan. 1993.

[27] C. Kurak and J. McHugh, "A cautionary note on image downgrading," in IEEE Computer Security Applications Conf., 1992, pp. 153–159.

[28] S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann, and D. Sobel,"Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," Rep. of a Special Panel of the ACM U.S. Public Policy Committee, June 1994.

[29] G. C. Langelaar, J. C. A. van der Lubbe, and J. Biemond, "Copy protection for multimedia data based on labeling

techniques," presented at the 17th Symp. on Information Theory in the Benelux, Enschede, The Netherlands, May 1996.
[30] N. F. Maxemchuk, "Electronic document distribution," AT&T Tech. J., vol. 73, no. 5, pp. 73–80, Sept./Oct. 1994.
[31] B. C. J. Moore, An Introduction to the Psychology of Hearing. New York: Academic, 1989.
[32] I. S. Moskowitz and M. H. Kang, "Covert channels—Here to stay?" Compass 94, pp. 235–243.
[33] R. M. Needham, private communication, Dec. 1995.
[34] T. Parson, Voice and Speech Processing. New York: McGraw-Hill,1986.
[35] B. Pfitzmann, "Information hiding terminology," in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, pp. 347–350,1996.
[36] "Trials of traced traitors," in Information Hiding, Springer Lecture Notes in Computer Science, vol. 1174, pp. 49–64, 1996.
[37] I. Pitas, "A method for signature casting on digital images," in Int. Conf. Image Processing, vol. 3, Sept. 1996, pp. 215–218.
[38] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions," DIMACS, Tech. Rep. 97-15, Apr. 1997.
[39] D. L. Schilling, Meteor Burst Communications: Theory and Practice.New York: Wiley, 1993.
[40] B. Schneier, Applied Cryptography—Protocols, Algorithms and Source Code in C, 2nd ed. New York: Wiley, 1995.