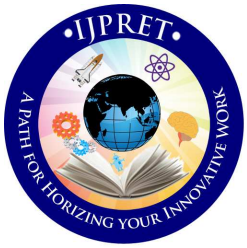
Research Article *ISSN: 2319-507X*
Rashmi Wakode, IJPRET, 2013; Volume 1(8):626-635 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ENHANCING IMAGE SECURITY THROUGH A COMBINATION OF TWO SHARES VISUAL CRYPTOGRAPHY, LSB STEGANOGRAPHY & WATERMARKING-A REVIEW

PROF. RASHMI A. WAKODE, PROF. M. D. INGOL, PROF. M. S. JOSHI

1. Asst.Prof.Electronics & Tele-communication Eng. IBSS Eng. Badnera(Maharashtra).
2. HOD, Electronics & Tele-communication Eng. PRMIT & R Badnera(Maharashtra).
3. Professor, Electronics & Tele-communication Eng. PRMIT & R, Badnera(Maharashtra).

Accepted Date:
27/02/2013
Publish Date:
01/04/2013

Keywords
Steganography,
Watermarking,
Cryptography,
Secret Communication,
Data hiding

Corresponding Author
Prof. Rashmi A. Wakode

Abstract

Now it is possible to enhance the Image Security over insecure channel by the combine use of a Cryptography, Steganography and watermarking techniques. Combinely Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. The Watermarking aims to validate the host and the undeniable identity of the legal owner. Steganography, Cryptography and watermarking individually provides security to the image, text and data but combine effect of all the three will provide robust system of protection to the image.

Introduction

Espionage, financial theft, infringement and cross border crimes are deterrent to social and legal systems which amass a great deal of secret and highly confidential information. High profile secrets if revealed can lead to disastrous confusion. Therefore with people's iniquity sky rocketing every day, the need to keep secrets as a secret for social and ethical needs has become all the more important. Most of the precedent algorithms have been mangled easily by hackers thus necessitating the quest for an impregnable algorithm. In this context, Steganography, Cryptography and Watermarking is used as a package to increase the degree of security in Image Protection which in turn is very hard to be hacked or cracked.

Comparison of Steganography, Cryptography and Watermarking:

Digital Steganography protect secrets by hiding information in video, audio, digital image, etc. Cryptography differs from Steganography in the sense that the former focuses on keeping the contents of a message secret through scrambling and its meaning meaningless, while the later focuses on keeping the existence of a message secret. Digital watermarking is the process of Embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners. In modern times Steganography and cryptography are complementary: first the message is encrypted and then is hidden using Steganography. Images are the most popular carriers for Steganography. Steganography and cryptography are both ways to protect information from intruders but neither technology alone is perfect and can be compromised. Two other technologies that are closely related to Steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than Steganography. The purpose of Steganography is partly defeated when the presence of hidden information is revealed or even suspected, however its strength can be aggrandized by combining it with cryptography and watermarking. By using the combination of two shares image cryptography,LSB Watermarking and

Steganography method ,on host side first the watermark is embedded in Image then, the obtained Image is divided in equal shares of black and white and after that a Steganography is used to hide secret message behind the cover image. The exact reverse process can be applied on the receiver side. Out of the numerous Steganography methods proposed, Least Significant Bits (LSB) substitution is the most popular and simple method that utilizes the least bits of a pixel in the cover image for embedding. The main reasons for the LSB Substitution method to be popular are as follows.

1. The ease of computation is very high because of its straight forward implementation.
2. Large amount of information or payload can be hidden in the cover image without distorting it.

Human eye is sensitive only to the changes made in the smooth areas of an image. It overlooks or cannot perceive the alterations made to the less sensitive edge areas of the image.

The LSB method is the simplest of all the methods and is used generally.

The figure next shows the above mentioned data security disciplines.

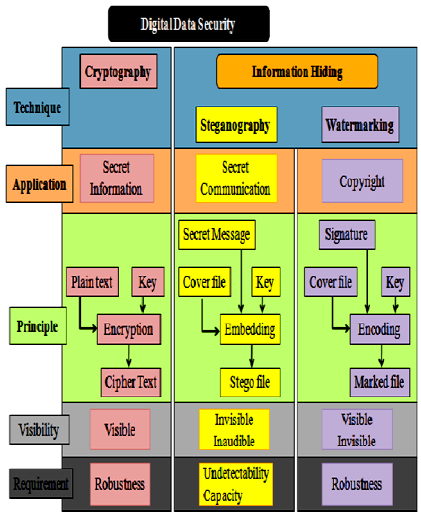


Figure 1*.Digital data security disciplines.

Steganography

Steganography can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of Steganography.

• Fragile

Fragile Steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not

been tampered with, such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile Steganography techniques tend to be easier to implement than robust methods.

• Robust

Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal would be easily perceived.

There are two main types of robust marking. Fingerprinting involves hiding a unique identifier for the customer who originally acquired the file and therefore is allowed to use it. Should the file be found in the possession of somebody else, the copyright owner can use the fingerprint to identify which customer violated the license agreement by distributing a copy of the file.

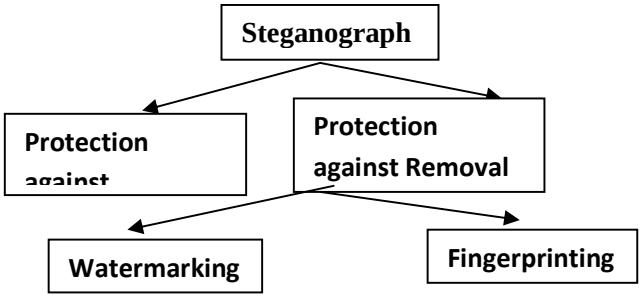


Figure 2*.Types of Steganography.

Taken from"An Analysis of Steganography Techniques" by Popa [2].

Steganography provides a means of secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data will be confidential unless an attacker can find a way to detect it.

Technique	Purpose	Security
Watermarking	Copyright/Authentication	90%
Cryptography	Security	90%
Steganography	Security	80%
Watermarking + Cryptography +Steganography	Authentication &Security	98 %

Figure 3*.Comparison of secret communication techniques.

Taken from "An Analysis of Steganographic Techniques" by Popa [2].

Image Watermarking: Digital watermarking is a method to hide some information that is integrated with a multimedia object [14]. The object may be any form of multimedia,

such as image, audio, video, or text. Watermarking has many different applications, such as ownership evidence, fingerprinting, authentication and integrity verification, content labeling and protection, and usage control. The success of any watermarking scheme is determined by its performance against intentional and unintentional attacks [9]. Any watermarking technique has to be evaluated to judge its performance.

Simple Watermarking:

A very simple yet widely used technique for watermarking images is to add a pattern on top of an existing image. Usually this pattern is an image itself - a logo or something similar, which distorts the underlying image.

Following figure shows the visible watermarking system:

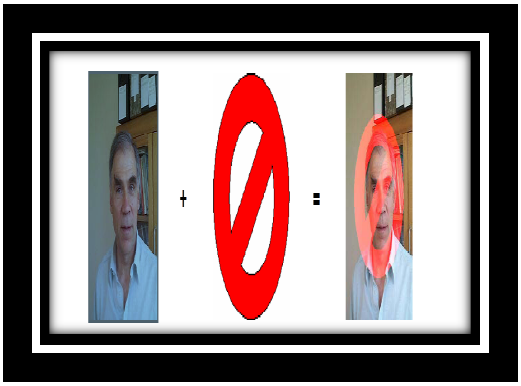


Figure 4*. Visible Watermarking

In the example above, the pattern is the red middle image while the portrait picture of Dr.Axford is the image being watermarked. In a standard image editor it is possible to merge both images and get a watermarked image. As long as you know the watermark, it is possible to reverse any adverse effects so that the original doesn't need to be kept. This method is only really applicable to watermarking, as the pattern is visible and even without the original watermark, it is possible to remove the pattern from the watermarked image with some effort and skill.

TYPES OF WATERMARKING

Digital watermarking is the process of Embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners. There are two types of digital watermarking as follows-

1) Visible Watermarking

2) Invisible Watermarking

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible

watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of watermarking,

5.VISUAL CRYPTOGRAPHY

Visual cryptography is the scheme where 2 shares are generated from the original secret image and by stacking together the secret is reveal [1,2]. This is the basic of the technique, however if we create more than 2 shares and some or all of them staked for getting the real secret is called visual secret sharing[3,4]. Following Figure shows the basic behind this scheme.

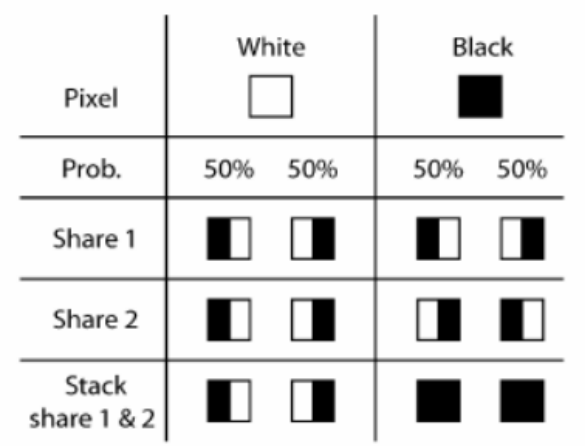


Figure 5*. Visual Cryptography

In this concept one white or black pixel will divide into two sub pixel. One way combination of the pixel division is shown in above Figure 5. It is mention that the shares 1 and 2 are stacked together and get the result in the form of complete black or gray (it's partially white and black but visualizes as gray). Because of this when we stacked the shares the white in original secret image become gray in the stacked result.

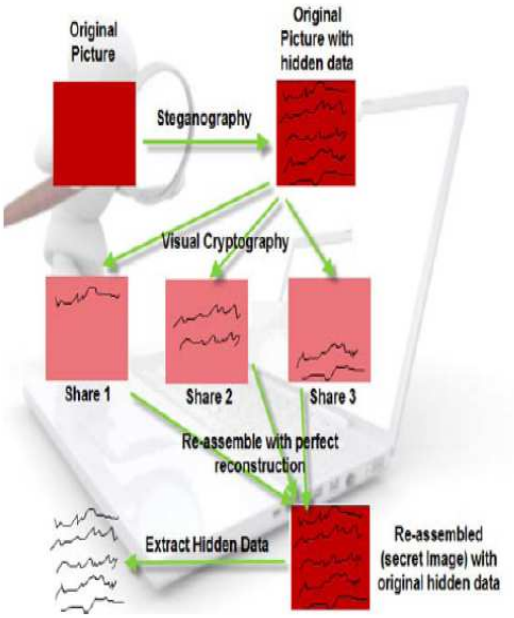


Figure 6*. Visual Cryptography(N-Share method)

In the above figure at the top left side the cover image is shown behind that the secret data is to be hide. After hiding the secret data the steno image is formed i.e. cover image + secret image or text. After performing Steganography cryptography is done there by creating the three shares. If one assembles these shares in a proper format, that person can get the re-assembled image.

Conclusion:

It can be concluded that when normal image security using Steganography and visual cryptography and watermarking technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the Steganography method is highly optimized using genetic algorithm. The proposed system is highly resilient against RS attack and optimally used for both grayscale and colored output in visual secret shares making it highly compatible for real-time applications. The future work could be towards the enhancing the algorithm using neural network for the visual watermarking, so that the system can generate highly undetectable secret shares using certain set of training data which might be automatically generated and is disposed after the task has been performed. Such type of approach might render the most secure Steganography, watermarked and visual cryptographic scheme.

Reference:

1. M. Naor, A. Shamir, "Visual Cryptography", Advances in Cryptography-Eurocrypt' 94, Vis Lecture Notes in Computer Science 950, PP.1-12.

2. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf , 1998

3. Young-Chang Hou, "Visual Cryptography for Color images", Pattern Recognition Society. Published by Elsevier Science Ltd.2003.

4. Ravindra Gupta, Akanksha Jain, Gajendra Singh, "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics", International Journal of Computer Science and Information Technology,Vol.3(3)"2012.

5. Anderson and Petitcolas Anderson, R., Petitcolas, "On the limits of the Steganography", IEEE Journal Selected Areas in Communications, Vol. 16(4), Page(s) 4,474-481, 2001.

6. Bassia et al. Bassia, P., Pitas, I., Nikolaidis N.: "Robust audio watermarking in the time domain", IEEE Transactions on Multimedia, Volume 3, Issue 2, and Page: 232 – 241, June 2001.

7. Cedric et al. Cedric, T., Adi, R., M cloughlin, "Data concealment in audio using a nonlinear frequency distribution of PRBS coded data and frequency-domain LSB insertion, Proc. IEEE Region 10 International Conference on Electrical and Electronic Technology, Kuala Lumpur, Malaysia, pp 275-278,2000.

8. Dumitrescu et al. 2002 Dumitrescu, S., Wu, W., Memon, N.: On steganalysis of random LSB embedding in continuous-tone images, Proc. International Conference on Image Processing, Rochester, NY, pp 641-644.

9. Fridrich et al. 2002 Fridrich, J., Goljan, M., Du, R.: (2002) Lossless Data Embedding New Paradigm in Digital Watermarking,

Applied Signal Processing, 2002, 2, pp 185-196.

10. Lee and Chen Lee, Y., Chen, L" High capacity image Steganography model", IEEE Proceedings on Vision, Image and Signal Processing, 147, 3, pp 288-294,2000.

11. Mintzer et al. Mintzer, F., Goertzil, G., Thompson, G.: "Display of images with calibrated color on a system featuring monitors with limited color palettes", Proc. SID International Symposium, pp 377-380, 1998.

12. Mobasseri, B.: "Direct sequence watermarking of digital video using m-frames, Proc", Chicago, IL, pp 399- 403.

13. Yeh, C., Kuo, C.: "Digital Watermarking through Quasi m-Arrays, Proc. IEEE Workshop on Signal Processing Systems", Taipei, Taiwan, 456-461. [Zwicker 1982] Zwicker, E.: Psychoacoustics, Springer Verlag, Berlin, Germany, 1999.

14. Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation, Convergence and Hybrid Information Technology", ICCIT'08.ThirdInternationalConference, 11-13, Volume: 2, pp: 539-544, Nov 2008.

15. K. Romani, E Prasad, S Varadarajan, "Stenography using BPCS to the integer wavelet transform", IJCSNS international journal of Computer science and network security, vol-7, No: 7 July 2007.

16. Ramani K.; Prasad E.V, Varadarajan S.; Subramanyam A,"A Robust Watermarking Scheme for Information Hiding", Advanced Computing and Communications, 16th International Conference, pp: 58 – 64, 14-17 Dec. 2008.

17. S. Joo, Y. Suh, J. Shin, H. Kikuchi, and S. J. Cho., "A new robust watermark embedding into wavelet DC components," ETRI Journal, 24, pp. 401-404, 2002.

18. Voloshynovskiy. S. S. Pereira and T. Pun. "Attacks on Digital watermarks: classification, Estimation-Based attacks and Benchmarks", Comm, Magazine. 39(8):118-126, 2001.

19. Mrs. kalavati Alla, Asst. Prof, Christu Jayanti Jubilee College, Dr. R. Siva Ram Prasad, Professor, Acharya Nagarjuna

University, “A Novel Hindi Text Steganography Using Letter Diacritics and its Compound Words”, IJCSNS International Journal Of Computer Science and Network Security,VOL.8 No.12,Dec 2008.

20. Vandana Tehlani, "A New Fragile Approach for Optimization in Invisible Image Watermarking by Using Symmetric Key Algorithms”, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012.

21. Ross J. Anderson, editor. “Information hiding: 1st international workshop, volume 1174 of Lecture Notes in Computerb Science, Isaac Newton Institute, Springer-Verlag, Berlin, Germany, May 1996.