SCITECH
RESEARCH ORGANISATION|
Volume 3, Issue 3
May 4, 2015|
Journal of Information Sciences and Computing Technologies
www.scitecresearch.com

Hiding Information- A Survey

Subhojit Malik[1], Writi Mitra[2]
[1] Assistant Professor, ECE Department, Hooghly Engineering & Technology College, Vivekananda Road, Pipulpati. P.O. & Dist.-Hooghly. West Bengal. India,
[2] Assistant Professor, ECE Department, Hooghly Engineering & Technology College, Vivekananda Road, Pipulpati. P.O. & Dist.-Hooghly. West Bengal. India,

Abstract

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. In order to address this Information Security, Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. This paper is a tutorial review of the steganography techniques appeared in the literature.

Keywords: Digital image steganography; spatial domain; frequency domain; adaptive steganography; security.

1. Introduction

For decades people strove to develop innovative methods for secret communication. The remainder of this introduction highlights briefly some historical facts and attacks on methods (also known as stegano analysis). A thorough history of steganography can be found in the literature [1, 2, 3]. Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines. The work presented here revolves around steganography in digital images and does not discuss other types of steganography (such as linguistic or audio).

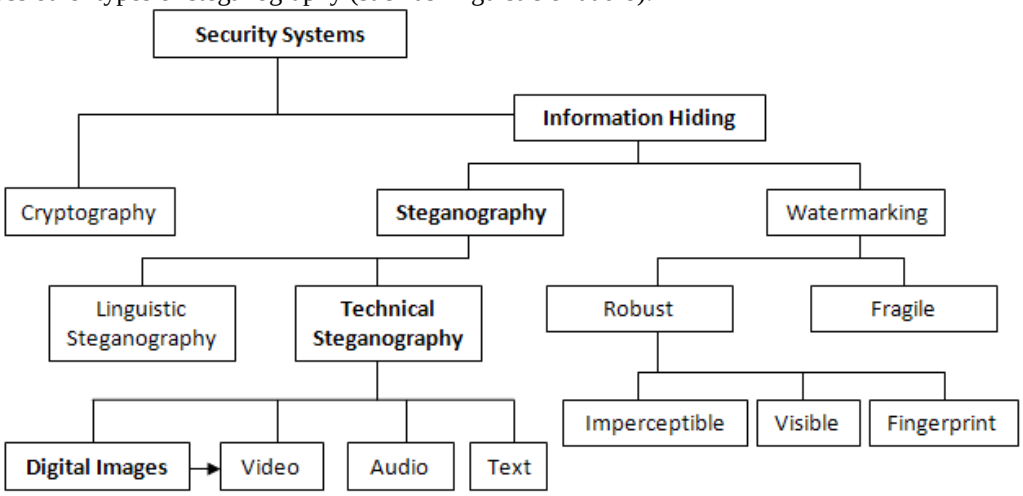

Fig. 1: The different embodiment disciplines of information hiding. The arrow indicates an extension and bold face indicates the focus of this study.

Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information .The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them.

Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it.

.

2. Review of Literature

The word steganography is originally derived from Greek words which mean "Covered Writing". It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [1, 2, 3, 4]. In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [5]. Five hundred years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text. It was also reported that the Nazis invented several steganographic methods during World War II such as Microdots, and have reused invisible ink and null ciphers. As an example of the latter a message was sent by a Nazi spy that read: "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils." Using the 2nd letter from each word the secret message reveals: "Pershing sails from NY June 1" [2, 6, 7].

The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15thcentury, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists.

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. In modern approach, depending on the nature of cover object, steganography can be divided into five types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

So, in the modern age so many steganographic techniques have been designed which works with the above concerned objects. More often in today's security advancement, we sometimes come across certain cases in which a combination of Cryptography and Steganography are used to achieve data privacy over secrecy. Various software tools are also available in this regard.

With the boost in computer power, the internet and with the development of digital signal processing (DSP),information theory and coding theory, steganography has gone "digital". In the realm of this digital world steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Contemporary information hiding is due to [8-9]. One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh [10], who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known now as image-based steganography. This paper's focus is on the review of steganography in digital images. For a detailed survey on steganographic tools in other media from a forensic investigator's perspective the reader is referred to [14].Steganography is employed in various useful applications, e.g., copyright control of

materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Other applications are video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users) [1], and also checksum embedding [11-15]. Petitcolas [16] demonstrated some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems. Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure. Miaou et al. [17] present an LSB embedding technique for electronic patient records based on bi-polar multiple-base data hiding. A pixel value difference between an original image and its JPEG version is taken to be a number conversion base. Nirinjan and Anand [18] and Li et al. [19] also discuss patient data concealment in digital images .In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Stegano analysis. Stegano analysis is a process in which a stegano analyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

3. Methodology

In this section, we will discuss different techniques or methods which are often used in image, audio and video steganography. Inspired by the notion that steganography can be embedded as part of the normal printing process. The process takes less than one second as the embedded data is merely 12 bytes. Hence, users will be able to use their cellular phones to capture encoded data. They charge a small fee for the use of their decoding software which sits on the firm's own servers. The basic idea is to transform the image colour scheme prior to printing to its Hue, Saturation and Value components (HSV), then embed into the Hue domain to which human eyes are not sensitive. Mobile cameras can see the coded data and retrieve it. This application can be used for "doctor's prescriptions, food wrappers, billboards, business cards and printed media such as magazines and pamphlets" [20], or to replace barcodes.

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways .Many techniques involve the modification of the layout of a text, rules like using every n-th character or the altering of the amount of white space after lines or between words. The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining knowledge of the secret key. To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention—those areas where there is a great deal of natural colour variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

Each of these techniques can be applied, with varying degrees of success.

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works well for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object.

In spatial domain methods a stegano grapher modifies the secret data and the cover medium in the spatial domain, which involves encoding at the level of the LSBs. This method although simpler, has a larger impact compared to the other two types of methods [26].

For example, if we consider image Steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it. The resultant image for the above data insertion and the original cover image are given below.

Fig. 2: The cover image

Fig. 3: The stego-image (after A is inserted)

Algorithm for embedding
Step 1: Start
Step 2: Read the cover audio file and the target Text message
Step 3: Normalize the cover audio in 16 bits.
Step 4: Store the length of the target message using standard LSB technique.
Step 5: Pre-process the Target secret message.
Step 6: Embed hexadecimal digits of pre-processed steps using modulo 16 operations and adjusting sample values based on forward and backward differences.
Step 7: Send the obtained Stego Audio to the receiver.
Step 8: End

Potdar et al. [27] used a spatial domain technique in producing a fingerprinted secret sharing Steganography for robustness against image cropping attacks. Their paper addressed the issue of image cropping effects rather than proposing an embedding technique. The logic behind their proposed work is to divide the cover image into sub-images and compress and encrypt the secret data. The resulting data is then sub-divided in turn and embedded into those image portions. To recover the data, a Lagrange Interpolating Polynomial was applied along with an encryption algorithm. The computational load was high, but their algorithm parameters, namely the number of sub-images (n) and the threshold value (k) were not set to optimal values leaving the reader to guess the values. Bear in mind also that if n is set to 32, for example, that means 32 public keys are needed along with 32 persons and 32 sub-images, which turns out to be unpractical. Moreover, data redundancy that they intended to eliminate does occur in their stego-image. Shirali-Shahreza, M. H. and Shirali-Shahreza, M. [28] exploited Arabic and Persian alphabet punctuations to hide messages. While their method is not related to the LSB approach, it falls into the spatial domain if the text is treated as an image. Unlike the English which has only two letters with dots in their lower case format, namely "i" and "j", Persian language is rich in that 18 out of 32 alphabet letters have dots. The secret message is binarized and those 18 letters' dots are modified according to the values in the binary file. Colour palette based steganography exploits the smooth ramp transition in colours as indicated in the colour palette. The LSBs here are modified based on their positions in the palette index. Johnson and Jajodia**[1]** were in favour of using BMP (24-bit) instead of JPEG images. Their next-best choice was GIF files (256-color). BMP as well as GIF based steganography apply LSB techniques, while their resistance to statistical counter attacks and compression are reported to be weak [3, 29, 30, 31, 32, 33]. BMP files are bigger compared to other formats which render them improper for network transmissions. JPEG images however, were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain. In **[33]**, the authors claimed that changes as small as flipping the LSB of one pixel in a JPEG image can be reliably detected. The experiments on the Discrete Cosine Transform (DCT) coefficients showed promising results and redirected researchers' attention towards this type of image. In fact acting at the level of DCT makes steganography more robust and less prone to statistical attacks.

Masking and filtering techniques are mostly used on24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected. Observe that the luminance in Figure 2 is at 15% in the mask region if it was decreased then it would be nearly invisible Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

Fig. 4: Masking

Patchwork and other similar tools do redundant pattern encoding, which is a sort of spread spectrum technique. It works by scattering the message throughout the picture. This makes the image more resistant to cropping and rotation. Smaller secret images work better to increase the redundancy embedded in the cover image, and thus

make it easier to recover if the stego-image is manipulated .The Encrypt and Scatter technique tries to emulate white noise. It is mostly used in image steganography. White Noise Storm is one such program that employs spread spectrum and frequency hopping. It does this by scattering the message throughout an image on eight channels within a random number that is generated by the previous window size and data channel. The channels then swap rotate, and interlace amongst each other. Each channel represents one bit and as a result there are many unaffected bits in each channel. This technique is a lot harder to extract a message out of than an LSB scheme because to decode you must first detect that a hidden image exists and extract the bit pattern from the file. While that is true for any stego-image you will also need the algorithm and stego key to decode the bit pattern, both of which are not required to recover a message from LSB. Some people prefer this method due to the considerable amount of extra effort that someone without the algorithm and stego-key would have to go through to extract the message. Even though White Noise Storm provides extra security against message extraction it is just as susceptible as straight LSB to image degradation due to image processing.LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF etc.JPEG images use the discrete cosine transform to achieve compression. DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT .In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV,AU, and even MP3 sound files [22-26].Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. The list of methods that are commonly used for audio steganography are listed and discussed below.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

4. Discussion

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Spies have used it since the time of the Greeks to pass messages undetected. Terrorists can also use steganography to keep their communications secret and to coordinate attacks. It is exactly this potential that we will investigate in the next section. Because you can hide information without the cover source changing, steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganographic methods can be used to hide this.

5. Conclusion

Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly. Since detection can never give a guarantee of finding all hidden information, it can be used together with methods of defeating steganography, to minimize the chances of hidden communication taking place. Even then, perfect steganography, where the secret key will merely point out parts of a cover source which form the message, will pass undetected, because the cover source contains no information about the secret message at all. In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide away of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. More restrictions on the use of privacy-protecting technologies are not very unlikely, especially in this period of time with great anxiety of terrorist and other attacks.

Acknowledgements

The authors would like to thank the Department of Electronics and Communication Engineering and the authority of Hooghly Engineering and Technology College, Hooghly, West Bengal, India for providing the facilities, support and continuous encouragement to continue research work. The authors would also like to thank Prof. Samir Kumar Bandyopadhyay, Calcutta University, India for his supervision and valuable guidance to carry out this work.

6. References

[1] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2) (1998) 26-34.

[2] J.C. Judge, Steganography: Past, present, future. SANS Institute publication,

http://www.sans.org/reading_room/whitepapers/stenganography/552.php, 2001.

[3] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, 01 (3)(2003)32-44.

[4] P. Moulin and R. Koetter, Data-hiding codes, Proceedings of the IEEE, 93 (12)(2005)2083-2126.

[5] S.B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE InternationalConference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.

[6] S. Lyu and H. Farid, stegano analysis using higher-order image statistics, IEEE Transactions on Information Forensics and Security, 1(1)(2006) 111-119.

[7] D. Kahn, The Codebreakers: The comprehensive history of secret communication from ancient times to the Internet, Scribner, December 5, 1996.

[8] J.P. Delahaye, 'Information noyée, information cache', Pour la Science, 229(1996)142-146. www.apprendre-en-ligne.net/crypto/stegano/229_142_146.pdf. [in French].

[9] G.J. Simmons, The prisoners' problem and the subliminal channel, in: Proceedings of Internationalconference on Advances in Cryptology, CRYPTO83, August 22-24, 1984, pp. 51-67.

[10] C. Kurak and J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference, 30 Nov-4 Dec, 1992, pp. 153-159.

[11] T.L. Thomas, Al Qaeda and the Internet: The danger of "cyber planning", Parameters, US Army War College Quarterly-Spring 2003. Available from:www.carlisle.army.mil/usawc/Parameters/03spring/thomas.pdf.

[12] C. Hosmer, Discovering hidden evidence, Journal of Digital Forensic Practice, (1)(2006)47-56.

[13] J.C. Hernandez-Castro, I. Blasco-Lopez and J.M. Estevez-Tapiador, Steganography in games: A general methodology and its application to the game of Go, Computers and Security, Elsevier Science, 25(2006) 64-71.

[14] P. Hayati, V. Potdar, E. Chang, A survey of steganographic and stegano analytic tools for the digital forensic investigator, available from:

http://debii.curtin.edu.au/~pedram/images/docs/survey_of_steganography_and_steganalytic_tools.pdf

[15] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, Applications for data hiding, IBMSystems Journal, 39 (3&4)(2000) 547-568.

[16] F.A.P. Petitcolas, "Introduction to information hiding", in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.)(2000) Information hiding techniques for steganography and digital watermarking, Norwood: Artech House,INC.

[17] S. Miaou, C. Hsu, Y. Tsai and H. Chao, A secure data hiding technique with heterogeneous data-combiningcapability for electronic patient records, in: Proceedings of the IEEE 22nd Annual EMBS International Conference, July 23-28, 2000, Chicago, USA, pp. 280-283.

[18] U.C. Nirinjan and D. Anand, Watermarking medical images with patient information, in: Proceedings of the20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 29 Oct-1 Nov, 1998, pp. 703-706.

[19] Y. Li, C. Li and C. Wei, Protection of mammograms using blind steganography and watermarking, in Proceedings of the IEEE International Symposium on Information Assurance and Security, 2007, pp. 496-499.

[20] D. Frith, Steganography approaches, options, and implications, Network Security, 2007(8)(2007)4-7.

[21] H. Farid, A Survey of image forgery detection, IEEE Signal Processing Magazine, 26(2)(2009)16-25.

[22] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, A secure and improved self-embedding algorithm tocombat digital document forgery, Signal Processing, 89 (12)(2009)2324-2332.

[23] N.F. Johnson and S.C. Katzenbeisser, "A survey of steganographic techniques", in: S. Katzenbeisser andF.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking ,Norwood: Artech House, INC.

[24] K. Bailey and K. Curran, An evaluation of image based steganography methods, Multimedia Tools and Applications, 30 (1)(2006) 55-88.

[25] [Hide and Seek]:

ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/cypherpunks/steganography/hdsk41b.zip

[S-Tools]: ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tools4.zip

[Stella] :http://wwwicg.informatik.uni-rostock.de/~sanction/stella/

[Hide in Picture]: http://sourceforge.net/projects/hide-in-picture/

[Revelation]: http://revelation.atspace.biz/

[Camouflage]: http://camouflage.unfiction.com/

[JpegX]: http://www.freewarefiles.com/Jpegx_program_19392.html

[Data Stash]: http://www.skyjuicesoftware.com/software/ds_info.html

[Other Tools]: http://www.jjtc.com/Security/stegtools.htm

[F5]: http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html

[OutGuess]: http://www.outguess.org/

[26] P. Alvarez, Using extended file information (EXIF) file headers in digital evidence analysis, International Journal of Digital Evidence, Economic Crime Institute (ECI), 2(3)(2004)1-5.

[27] V.M. Potdar, S. Han and E. Chang, Fingerprinted secret sharing steganography for robustness against image cropping attacks, in: Proceedings of IEEE 3rd International Conference on Industrial Informatics (INDIN),Perth, Australia, 10-12 August 2005, pp. 717-724.

[28] M.H. Shirali-Shahreza and M. Shirali-Shahreza, A new approach to Persian/Arabic text steganography, in: Proceedings of 5th IEEE/ACIS International Conference on Computer and Information Science (ICISCOMSAR2006), 10-12 July 2006, pp. 310-315.

[29] E.T. Lin and E.J. Delp, A review of data hiding in digital images, in: Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS'99, the Society for Imaging Science and Technology, 1999, pp. 274-278.

[30] C.C. Chang, C.Y. Lin and Y.Z. Wang, New image steganographic methods using run-length Approach, Information Sciences, 176 (22)(2006) 3393-3408.

[31] R.J. Hwang, K.T. Shih, C.H. Kao and T.M. Chang, Lossy compression tolerant steganography, in: Proceedings of the 1st International Conference on The Human Society and the Internet-Internet Related Socio-Economic Issues, Lecture Notes In Computer Science, 2001, vol. 2105, pp. 427-435.

[32] X. Kong, Z. Wang and X. You, stegano analysis of palette images: Attack optimal parity assignment algorithm, in: Proceedings of 5th IEEE International Conference on Information, Communications and Signal Processing, 06-09 Dec 2005, pp. 860-864.

[33] J. Fridrich, M. Goljan and D. Hogeg, stegano analysis of JPEG images: Breaking the F5 algorithm, in: Proceedings of Information Hiding: 5th International Workshop, IH 2002 Noordwijkerhout, The Netherlands, LNCS, Springer, October 7-9, 2002, 2578/2003, pp. 310-323

1. List of abbreviations

The list of abbreviations which are used in the text, are given below:

LSB – Least Significant Bit

DCT – Discrete Cosine Transform

JPEG – Joint Photographic Experts Group

BMP - BitMap

GIF – Graphics Interchange Format

HSV – Hue Saturation Value

DSP – Digital Signal Processing

TCP/IP – Transmission Control Protocol/Internet Protocol

Authors' Biography

	Prof. Subhojit Malik is an Assistant Professor in the Department of Electronics & Communication Engineering, Hooghly Engineering & Technology College. He has a Master Degree in Intelligent Automation and Robotics from Jadavpur University, Kolkata,India and his areas of interest are Intelligent Automation, Digital Signal Processing and Image Processing.
	Prof. Writi Mitra is an Assistant Professor in the Department of Electronics & Communication Engineering, Hooghly Engineering & Technology College. She has a Master Degree in Digital Systems & Instrumentation from IIEST,Shibpur,India and areas of interest are VLSI Design, Digital Signal Processing and Image Processing.