IMAGE ENCRYPTION USING LSB

[1]Shubham Tripathi, [2]DilipYadav, [3]Ankur Kumar
Department of Electrical Engineering
[1,2] Sraoj Institute of Management & Technology, Lucknow
[3]Shri Ram Group of Colleges, Muzaffarnagar UP, India
shubhamvtripathi06@gmail.com
dilip1987kumar@gmail.com
ankurdhiman07@gmail.com

Abstract: **This paper confers about how digital images can be used as a carrier to fleece messages. Steganography has been highlighted as the better way of fortifying messages than cryptography which only conceals the content of the messages not the existence of the message. Original message is hidden within a carrier such that the changes so occurred in the carrier are not observable. LSB is a more robust technique that takes advantages of the strengths and circumvents the limitations. It is investigated that the text is concealed behind an image without any distortion in the image. Whereas, hiding an image within an image results trivial distortion in the image.**

Keywords***:*** **Cryptography; Image; Steganography; Least Significant Bit (LSB).**

I. Introduction

INFORMATION hiding, steganography, and watermarking are three thoroughly correlated fields that have a prodigious deal of overlap and share many technical tactics. However, there are fundamental philosophical alterations that affect the requirements, and thus the design, of a technical solution. Steganography is invented by Trithemius [1]. The term derived from the Greek words steganos, which means “covered,” and graphia, states “writing.” Steganography distinct as the art of covered communication. Secrecy of steganography is more sensible with the written codes, besides imperceptible ink an oft-cited instance of steganography elucidated in an ancient story from Herodotus. As per story a slave sent by his master, named Histius, to the Ionian city of Miletus with a secret message tattooed on his scalp. After tattooing, the slave grew his hair back in order to conceal the message. He then voyaged to Miletus and, upon arriving, shaved his head to reveal the message to the city’s regent, Aristagoras. In this situation, the message is of primary value to Histiaeus and the slave is simply the transporter of the message.

These assertions climaxes the alteration between steganography and watermarking. Envisagethe message on the slave’s skull read, “This slave belongs to Histiaeus.” In that this message refers to the slave (cover work), this would encounter our definition of a watermark, maybe the only reason to secrete the message would be enhancing. However, if someone else requested possession of the slave, Histiaeus could shave the slave’s head and verify possession. In this scenario, the slave (cover work) is of key value to Histiaeus, and the message offers useful evidence about the cover work [4]. Systems for introducing messages in works can thus be separated into watermarking systems, in which the message is related to the cover Work, and non-watermarking systems, in which the message is unrelated to the cover work. They can also be self-reliantly divided into steganographic systems, in which the very reality of the message is kept underground, and non-steganographic systems, in which the presence of the message need not be secret.

The steganography can be more exactly elucidated by several incidents in history. In 1981, photographic reprints of private British cabinet papers were being printed in newspapers. Rumour has it that to regulate the source of the leak. Margaret Thatcher arranged to issue uniquely recognisable copies of documents to each of her ministers. Each copy had a diverse word arrangement that was used to encrypt the distinctiveness of the recipient. In this way, the source of the escapes could be recognized. This is an example of covert watermarking. The watermarks prearranged info related to the beneficiary of each copy of the documents, and were concealed in that the ministers were kept unaware of their existence so that the foundation of the leak could be identified. The leeway of steganographically rooted data unrelated to the cover work (i.e., messages hidden in otherwise innocuous transmissions) has always been a concern to the military. Simmons delivers a captivating explanation of covert channels, where the technical issues surrounding confirmation of the SALT-II treaty among the United States and the Soviet Union has been conversed. The SALT-II treaty allowed both countries to have many missile storage but only a partial quantity of missiles. To verify consent with the treaty, each country would install sensors, provided by the other country, in their silos. Each sensor would tell the other country whether or not its silo was engaged, but nonentity else. The concern was that the corresponding countries might design the sensor to interconnect supplementary information, such as the location of its storage, concealed confidential the honest message [7].

II. LITERATURE ANALYSIS

Although the art of papermaking was conceived in China over one thousand years earlier, paper watermarks did not seem until about 1282, in Italy. The marks were finished by adding thin wire outlines to the paper moulds. The paper would be marginally thinner where the wire was and hence more clear. The meaning and purpose of the initial watermarks are indeterminate. They may have been used for applied functions such as classifying the mildews on which sheets of papers were made, or as symbols to recognise the paper maker. On the other hand, they may have represented spiritual signs, or might simply have attended as beautification. By the eighteenth century, watermarks on paper made in Europe and America had become more clearly practical. They were used as symbols, to record the date the paper was manufactured, and to designate the sizes of unique sheets. It was also about this time that watermarks began to be used as ant forging measures on money and other documents. The term watermark seems to have been invented near the end of the eighteenth century and may have been resulting from the German term Wassermarke. The term is actually a contradiction, in that water is not particularly important in the conception of the mark. It was possibly given because the marks resemble the effects of water on paper [5].

About the time the term watermark was invented, forgers began developing methods of forging watermarks used to defend paper money. In 1779, Gentleman's Magazine reported that a man named John Mathison had exposed a method of forging the water-mark of the bank paper, which was before believed the major security against frauds. This finding he made a suggestion to disclose, and of instruction the world the method of detecting the fraud, on disorder of pardon, which, however, was no weight with the bank. John Mathison was hanged. Forging encouraged advances in watermarking technology [4].

William Congreve, an Englishman, conceived a practice for making colour watermarks by introducing dyed material into the mid of the paper during papermaking. The resulting marks must have been tremendously difficult to forge, because the Bank of England itself deteriorated to use them on the grounds that they were too difficult to make. A more applied technology was created by another Englishman, William Henry Smith. This substituted the fine wire designs used to make earlier marks with a category of shallow respite sculpture, pressed into the paper mould [11]. The resulting variation on the surface of the mould shaped beautiful watermarks with variable shades of grey. This is the basic technique used today for the face of President Jackson [12].

Two projects backed by the European Union, VIVA and Talisman, tested watermarking for transmission monitoring. The International Organization for Standardization took an attention in the technology in the setting of scheming advanced MPEG standards. In the late 1990s numerous companies were recognised to market watermarking products. Technology from the Verance Corporation was accepted into the first phase of SDMI and was used by Internet music distributors such as Liquid Audio. In the area of image watermarking, Digimarc hustled its watermark embedders and detectors with Adobe's Photoshop. More recently, a quantity of companies have used watermarking technologies for a variability of applications [9].

A. Literature of steganography

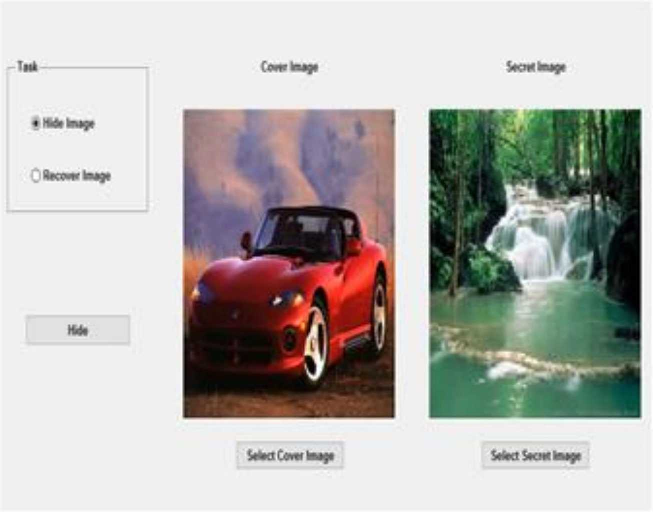
The first written indication about steganography being used to send message is the Herodotus story about slaves and their shaved heads previously mentioned. Herodotus also documented the story of Demeratus, who warned Sparta about the planned invasion of Greece by the Persian Great King Xerxes. Demeratus frayed the wax off the surface of a wooden script tablet and scratched his cautionary into the wood. The tablet was then covered with a fresh layer of wax to appear as a blank writing tablet that could be safely carried to Sparta without touching misgiving. Aeneas the Tactician projected many steganographic techniques that could be considered "state of the art" of his time, such as hiding messages in women's earrings or messages accepted by pigeons. He also defined several methods for walloping in text-by modifying the height of letter strokes or marking letters in a text using small holes Linguistic steganography, also called acrostic. It was one of the most popular ancient steganographic methods. Secret messages were programmed as preliminary letters of sentences or successive tercets in a poem. A more progressive version of language steganography originally perceived in China and reinvented by Cardan is the famous Cardin's Grille. The letters of the secret message do not form a regular structure but a random pattern "Th" is read simply by insertion a mask over the text. The mask is an early example of a secret (stego) key that had to be shared between communicating parties. Acrostic was also used in World War I by both the Germans and Allies. A precursor of modern steganographic methods was labelled by Francois Bacon. Bacon used italic or standard fonts to encode binary depictions of letters in his works. Five letters of the cover work could hold five bits and thus one letter of the alphabet. A modern form of this steganographic technique was labelled by Brassi. They used the feature that while shifting lines of text up or down by 1/300 of an inch is not visually noticeable, these small variations are vigorous enough to endure photocopying. Another idea that frolicked a significant part wars in the nineteenth and twentieth centuries was originally proposed by Brewster. He suggested hiding messages by shrinking them so much that they started resembling specs of dirt. The reduction was made conceivable by the technology developed by French photographer Dragon through the Franco-Prussian War. Microscopic images could be concealed in nostrils, ears, or under fingernails. In World War I, Germans used such "microdots" and hid them in corners of postcards slit open with a knife and resealed with starch. The modern twentieth-century microdots could grip up to one page of text and even contain photographs. The Allies discovered the use of microdots in 1941.

A more current and quite clever use of steganography helped Commander Jeremiah Denton convey the truth about his North Vietnamese captors. When walked in front of the news media as part of staged propaganda, Denton blinked his eyes in Morse code spelling out TORTURE [10].

Similar to watermarking, the prosperous of steganography accords with the arrival of the Internet. The quick spread of computer networks and change to digitization of media shaped a very positive environment for secret steganographic communication. Recently, steganography has been supposed as a conceivable means of information exchange and planning of terrorist bouts. It is only normal that such technology by its very nature could be used for planning criminal doings. Moreover, as of writing this book in mid-2006, there are over 300 steganographic products on the Internet accessible for download today. Some of these tools bid strong encryption approaches that encrypt the secret messages to provide an supplementary deposit of security in case the steganographic scheme is broken. Advances in steganography have urged the balancing field of steganalysis that started developing more rapidly after the terrorist attacks of September 11, 2001. Steganalysis is worried with developing methods for detecting the presence of secret messages and eventually extracting them. Steganography is considered broken even when the mere presence of the secret message is detected.

B. Importance of steganography

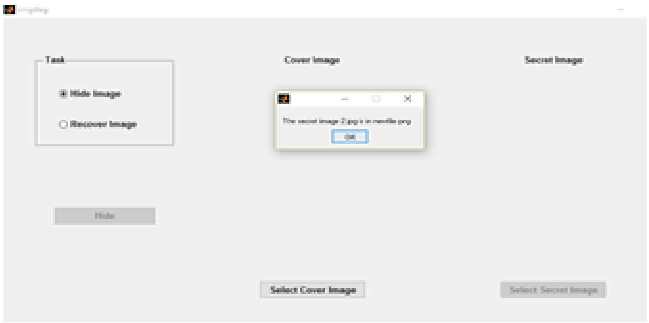
Electronic communication is progressively vulnerable to snooping and hateful interferences. The subjects of security and privacy have conventionally been loomed using tools from cryptography. Messages can be affixed with a message verification code (hash) and encrypted so that only the rightful receiver can read them and confirm their honesty and legitimacy. Modern cryptography is an established field based on demanding mathematical basics and decades of development. Encrypted messages are obvious, and when interrupted, it is clear that the sender and the receiver are communicating clandestinely. Steganography is the little and much younger sister of cryptography. It is a substitute tool for privacy and security. Instead of encrypting messages, one can pelt them in other inoffensive observing objects so that their very occurrence is not exposed. Thus, steganography can be a possible substitute in countries where usage of encryption is illegal or in domineering governments where using cryptography might entice unwanted attention. As cryptanalysis is the other side of the cryptography coin, so steganalysis is an inseparable part of steganography. Indeed, one perhaps cannot develop a good steganographic technique without expenditure a considerable amount of time on how to break it. The need for reliable steganalytic tools capable of detecting concealed messages has recently increased due to subjective evidence that steganography is being used by terrorists and child pornographers[15].



III. RESULT AND DISCUSSION

All of the approaches to steganography have one thing in common that they hide the secret message in the physical object which is sent. The following figure shows the steganography process of the cover image being passed into the embedding function with the message to encode resulting in a steganographic image containing the hidden message.

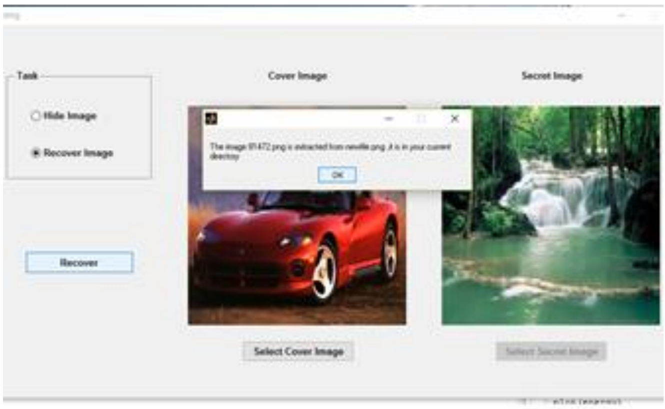
A key is often used to protect the hidden message. This key is usually a password, so this key is also used to encrypt and decrypt the message before and after the embedding



The secret image 2.jpg is in newfile.png

Figure 2: Encrypted image

Figure 1: Hiding of Image



The image 81472.png is extracted from newfile.png. It is in your current directory

Figure 3: Recover Image

IV. Conclusion

A better way of securing messages than cryptography which only conceals the content of the messages not the existence of the message. Original message is hidden within a carrier such that the changes so occurred in the carrier are not observable. LSB is a more robust technique that takes advantages of the strengths and avoids the limitations.It is investigated that the text is hidden behind an image without any distortion in the image i.e the stego image is exactly similar to the original image.While hiding an image within an image there is some amount of distortion in the image.

References

1. Hassan Mathkour, Batool al-sadoon,AmeurTouir.A new image steganography technique.In 978-1-4244-2108-4/08/2008 IEEE.
2. K.B Raja,C.RChowdary,Venugopal K.R,L.M Patnaik.In 0-7803-9588-3/05/2005 IEEE.
3. R.Chandramouli,NasirMemon.Analysis of LSB bsed technique. In 0-7803-6725-1/01/2001 IEEE.
4. K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik. Authentication of Secret Information in Steganography.In February 10, 2010 at 05:14 from IEEE.
5. MamtaJuneja ,Parvinder Singh Sandhu. Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption.In February 10, 2010 at 05:12 from IEEE.
6. HosseinMalekmohamadi and ShahrokhGhaemmaghami. Reduced complexity enhancement of steganalysis of lsb-matching image steganography. 978-1-4244-3806-8/09/$25.00 © 2009 IEEE.
7. H. A. Rahmel. System for determining the listen habits of wave signal receiver users. United States Patent, 2,513,360, 1950.
8. J. Simpson and E. Weiner, editors. Oxford English Dictionary. Oxford University Press, 2000.
9. David Kahn. The Codebreakers—The Story of Secret Writing. Scribner, New York, 1967.
10. J. J. Hernandez, F. Perez-Gonzalez, J. M. Rodriguez, and G. Nieto. Performance analysis of a 2D multipulse amplitude modulation scheme for data hiding and watermarking still images. IEEE Journal of Selected Areas in Communication, 16(4):510–524, 1998.
11. W. Szepanski. A signal theoretic method for creating forgery-proof documents for automatic verification. In J. S. Jackson, editor, 1979 Carnahan Conf. on Crime Countermeasures, pages 101–109, 1979.
12. R. Anderson, editor. Information Hiding, volume 1174 of Lecture Notes in Computer Science. Springer-Verlag, 1996.
13. G. Depovere, T. Kalker, J. Haitsma, M. Maes, L. de Strycker, P. Termont, J. Vandewege, A. Langell, C. Alm, P. Norman, B. O'Reilly, G. Howes, H. Vaanholt, R. Hintzen, P. Donnelly, and A. Hudson. The VIVA project: Digital watermarking for broadcast monitoring. IEEE Int. Conf. on Image Processing, 2:202–205, 1999.
14. Frank Hartung and Martin Kutter. Multimedia watermarking techniques. Proc. IEEE, 87(7):1079–1107, 1999.
15. T. Sharp. An implementation of key-based digital signal steganography. In I. S. Moskowitz, editor, Information Hiding, 4th International Workshop, IHW 2001, Pittsburgh,PA, April 25–27, 2001, volume 2137 of LNCS, pages 13–26. Springer-Verlag, New York, 2001.