AN IMPROVED LEAST SIGNIFICANT BITS USED FOR INFORMATION HIDING

Ms Manisha Verma
Assistant Professor(CSE),
Doon Business School, Dehradun, UK ,India
mankiishaverma@gmail.com

ABSTRACT

An improved Least Significant Bits (LSB) information hiding is proposed according to Secure Data Splitting Algorithm and Data Embedding Algorithm and based on this, quality will be managed by PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error) control monochromic images. So mainly what we are going to do is that an effort has been made to propose and implement a new steganographic technique for images by modifying existing algorithms. This technique uses LSB steganography as our basis and disperses a secret message over the entire image taken by us to ensure that the secret message cannot be get from the image. When we compare with other existing algorithms, we can easily prove that the difficulty of decoding the proposed algorithm is high

Keywords: Steganographic, PSNR,LSB,Cryptography

1. Introduction

Among different kinds of the carrier media, digital images are the most popularly used data on the Internet. A host image used to hide the secret data is called the cover image or the carrier image. When the secret data has got embedded into the cover image, the resultant image is called the stego image. Good stego image quality can avoid arousing suspicion during data transmission. In terms of the processing domain, image hiding schemes can be classified as either spatial-domain or frequency-domain image hiding schemes. Methods in the spatial domain embed secret data into cover pixels directly.One simple method is least significant bits (LSB) substitution. Methods in the frequency-domain transform each cover pixel from the spatial domain to the frequency domain. Then, the secret data are embedded into the transformed coefficients. In general, methods in the spatial domain get higher hiding capacities but low robustness, and vice versa. Previous image hiding schemes embed the secret into the digital image, and only people with the correct key can extract and decode the secret from the embedding image. If more than one person wants to share the secret, well, previous image hiding schemes cannot do anything about it.

1.1 Research Motivation

Security has become an inseparable issue as information technology is ruling the world now. Cryptography is the study of mathematical techniques related aspects of Information Security such as confidentiality, data security, entity authentication and data origin authentication, but it is not the only means of providing information security, rather one of the techniques. Visual cryptography is a new technique which provides information security which uses simple algorithm unlike the complex, computationally intensive algorithms used in other techniques like traditional cryptography. This technique allows Visual information (pictures, text, etc) to be encrypted in such a way that their decryption can be performed by the human visual system, without any complex cryptographic algorithms. This technique encrypts a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies. In this paper we provide an overview of the emerging Visual Cryptography (VC) and related security research work done in this area.

In recent years digital image-based steganography has established itself as an important discipline in signal processing. That is due in part to the strong interest from the research community. Unfortunately, given the high volume of the introduced techniques, the literature lacks a comprehensive review of these evolving methods.
All of the existing methods of steganography focus on the embedding strategy and give no consideration to the pre-processing stages, such as encryption, as they depend heavily on the conventional encryption algorithms which obviously are not tailored to steganography applications where flexibility, robustness and security are required. Andreas Westfield, a steganography scholar at Dresden University, called upon researchers in the field to analyze the interaction between steganography and encryption, the crypto-stego interface. Many of the current methods take for granted that resilience to

noise, double compression, and other image processing manipulations are not required in the steganography context. As such, in the warden passive attack scenario their hidden data will be destroyed or will not be retrievable.
Adaptive steganography aimed at identifying textural or quasi-textural areas for embedding the secret data runs into a few problems at the decoder side since its classification algorithms are not salient. In this thesis, skin-tone areas are the preferred choice for texture detection since the detection algorithm is robust and unique.Moreover, skin-tone areas always exhibit chrominance values residing along middle range, therefore, the problem of underflow or overflow is overcome automatically. In the process of searching for a good skin-tone detection algorithm, the various available techniques are proven to either be slow in execution and/or come with intolerable false alarms. Often, these algorithms neglect the fact that luminance can help improve their performance

1.2 Research Objective

1. Study the Data Hiding techniques by using Visual Cryptography techniques and their Noise and how to improve PSNR.
2. Develop the basic procedure for Least Significant Bit Algorithm (LSB).
3. Analyze the performance of proposed methods in terms of Visual Cryptography robustness of the steago image using PSNR calculations.
4. Implement the LSB method to analysis of PSNR.
5. Algorithm results based on LSB method using MAT Lab Simulation.

1.3 Research Contribution

This research work focuses on the tradeoff analysis of data hiding by using visual cryptography for gray-scale images using Least Significant Bit (LSB) and design, implement and improve PSNR using Least Significant Bit (LSB) by proposing methods of embedding and extracting the digital image. This consists of secret image embedding, attacks and secure data extraction. The performances of proposed methods will evaluate in terms of quietness and robustness. Experimental results of the proposed methods' performance will analyze using Peak Signal to Noise Ratio (PSNR) calculations.

There are a number of algorithms or transformations are used in Visual Cryptography for robustness, but we will use the LSB method and calculate the PSNR for robustness.

2. Cryptography

Cryptography is the science of writing in secret code the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Cryptography is the art of achieving security by encoding messages to make them non-readable. It is thescience of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is thescience of securing data, cryptanalysis is the science of analyzing and breaking secure communication.

Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience,determination, and luck. Cryptology embraces both cryptography and cryptanalysis.

Cryptography is study of mathematical technique to provide the methods for information security. It provides such services like authentication, data security, and confidentiality. Visual cryptography is one of the techniques used in modern world to maintain the secret massage transmission.

Visual cryptography is based on the images and is obtained by sending pixel information. Visual

Cryptography schemes depend on sub-pixels and its complexity, computation, reliability, etc. The image consistsof black and white, grayscale color images. Visual cryptography uses participates to send secret information.

2.1 Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) tobe encrypted in such a way that the decryption can be performed by humans (without computers). The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by

printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image.

Basic visual cryptography is based on breaking of pixels into some sub pixels or we can say expansion of pixels. Fig 2 shows two approaches for (2, 2) –Threshold VCS. In this particular figure first approach shows that each pixel is broken into two sub pixels. Let B shows black pixel and T shows Transparent (White)pixel. Each share will be taken into different transparencies. When we place both transparencies on top of each other we get following combinations, for black pixel BT+TB=BB or TB+BT=BB and for white pixel BT+BT=BT or TB+TB=TB. Similarly second approach is given where each pixel is broken into four sub pixels. We can achieve 4C2 =6 different cases for this approach.

2.2 Information hiding

While all the above mentioned cryptosystems have solved the problem of protecting privacy of information content they have not protected the anonymity of its sender and receiver In fact when data is encrypte dits random nature looks strange enough to make it stand apart from normal communications. Thus it perfectly reveals then encrypted communication is taking place between the two parties. In some other cases just leaking the existence of communication is enough to render the system unusable For example when the drug criminals hear the encrypted communication of the police over cellular phones in the region they will immediately stop and escape to other regions In such cases it is clear that the police wants its communication to be hidden from the drug criminals In another case when some vehicle starts its encrypted communication its exact location can be immediately calculated with two directional radars In network security the corresponding problem is called the tracanalysis problem Information hiding is not only used in military and police contexts but it isalso needed in the commercial world. A company needs to protect its vital financial documents. It can do sofor example by programming the word processor to hide its identification number in each electronic copy as well as hard copies of every document. Laterif a document is found leaked to another place i.e in the news media or at acompeting company the leakage can be traced back to its originator This is known as the tracing traitors problem.

For an abuse of this see e.g. as digital audio and video content is going to be more dominant over the analog one copyright protection is also a more serious problem When the information is digitalized the price of making a copy goes almost to zero In fact with a computer and a few commands everyone can copy the whole content of a CD or DVD to a magnetic tape a hard disk or to another CD or DVD In the case of the Internet the Web it is even easier Without any high tech skillanyone can choose to download and save an image or music clip with only a mouse click away.

Several solutions have been proposed to prevent this but few if any seems to protect the copyright perfectly while still maintaining the quality of the original document Companies such as IBM Sony Microsoft and AT&T have started collaborating together in seeking ways to hide copyright information into music and video This copyright information can later be checked by viewing or copying devices. Thus an important requirement for the hiding operation is that it must retain the high quality of the mediaat least in the perception of the viewers and listeners.

There is another application of information hiding In many countries where the use of cryptography are conditional or controlled individual users still want to protect their privacy but would not want to be noticed In such cases information hiding gives a satisfactory answer to the problem. It hides information to be sent into normal communication. If the hiding is perfect then even the existence of the secret communication is undetectable thus privacy of the communication is maximallyprotected.

A covert channel by its definition is hiding information into other unusual channelsthat were not designed to be communication channel. For instance current CPUor disk loadetc can be used as a mean of communication among users or processesin a computer system.

3. Comparison between Steganography and Cryptography

3.1 Cryptography

The word originates from Greek, which means "hidden, secret". Cryptography is the art of hiding the contents of a message from an attacker, but do not hide the existence of the message. It is affiliated closely with information theory, computer security and engineering.Cryptography hides the content of the message, but not the existence of the message; Steganography& watermarking hide both the contents and existence of the message.In modern days, cryptography techniques are used in credit cards, ATM cards, computer passwords and e-commerce, just to name a few.

3.2 Steganography

The term "Steganography" comes from Greek, which means "covered, hidden writing".Steganography performs message hiding such that an attacker cannot detect the presence of the message in the image/video/audio; watermarking hides the message such that an attacker cannot tamper with the message contained within the image/video/audio.Steganography is

hidden writing. The message is there, but nobody notices it. However, once noticed, it can be read. In modern times, steganography techniques include invisible inks, microdots (used by modern HP and Xerox color laser printers where tiny yellow dots containing printer serial number, date and time stamp, are added to each page), and digital watermarks.

4. RELATED WORK

Niels Provos [1] has explored a model to balance statistical properties of the cover image after embedding the pay load. Anderson et.al [2] has proposed a LSB based algorithm in which the quality of the retrieved image is poor. The two mathematical frameworks for Steganography, i.e. information theoretical model [3] and complex-theoretical view [5] give better mathematical foundations for applied steganography. A DCT co-efficient algorithm in which MSBs of hidden image are embedded into insignificant DCT coefficients of the cover image is presented in [6]. The usage, advantages, and limits of existing steganography techniques are analyzed in [7]. Aura [8] proposes that gray scale images are the best cover images.

He observes that uncompressed scans of images obtained with a digital camera with good resolution are

the safest image for steganography. Fredrich et.al, [9] conclude that the cover images stored in the JPEG format are a very poor choice for steganography that works in spatial domain, since very small modifications of the image can be reliably deleted by flipping the LSB of one pixel. Eggers et.al [10] observed that raw uncompressed format provides large space for secured steganography, but exchange of this uncompressed image is considered equivalent to cryptography by the same authors.

5. Least Significant Bit (LSB) Embedding

Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image.

In 8 bit images, one bit of information can be hidden. The cover image is shown in Figure 1(a) and a hidden image is shown in Figure 1(b). A stego-image is obtained by applying LSB algorithm on both the cover and hidden images (Figure 1(c)). The hidden image is retrieved from the stego-image by applying the reverse process (Figure 1(d))

Information hiding is a method of hiding secret data into a host medium so that the hidden data are imperceptible but known to the intended recipient. The host medium may be a digital image, audio, video, or another type of media. Among the different kinds of media, the digital image is most popularly used as the host media to convey secret information. In the image hiding system, the image used to embed secret data is called the host image (cover image). The resultant image, which is embedded with secret data, is called the stego-image.
Different approaches to data hiding have been proposed for different goals, such as, invisibility, robustness and capacity. One of the common approaches is based on manipulating the least-significant-bit (LSB) planes, which replaces the least significant bits of the host image with secret data. LSB approaches typically achieve high capacity.

In a data hiding procedure, the host image must not be degraded too much, otherwise the quality of the stego-image will not be acceptable, and the embedded data easily detected. A simple LSB substitution, which hides secret data into LSBs directly, is easy implemented but will result in a low quality stego-image. In order to achieve a good quality stego-image, Wang et al. used a substitution matrix to transform the secret data values prior to embedding into the host image. For a *k*-bit LSB substitution, the exhaustive search method would take a long period of time to find an optimal substitution matrix. In order to overcome a long running time of the exhaustive search, Wang *et al*. proposed a genetic algorithm to search for an approximate solution, and Chang *et al*. also proposed a dynamic programming strategy to find an optimal substitution matrix in an efficient manner.

6. PROBLEM STATEMENT

Problem definition: Given a cover image c and the image to be embedded (payload) h; the objective is,
(i) To embed the payload in the cover image by replacing LSB bits of cover image by the image of the payload. The combined image is called stego-object(s).
(ii) To transform the stego-object from spatial domain to frequency domain using DCT.
(iii) To compress the frequency domain stego-object using quantization and run length coding to generate a secure stego object.

REFERENCES

1. Alfred J, M et al., 1996.
2. Hand book of applied Cryptography.
3. First edn.Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the DiscreteWavelets Transform and Singular Value Decomposition, European Journal Of Scientific Research ,vol 39(1), pp 231-239.
4. Amirthanjan,R. Akila,R&Deepikachowdavarapu, P., 2010. A Comparative Analysisof Image Steganography, International Journal of Computer Application , 2(3), pp.2-10.
5. Arnold, M. 2000. Audio watermarking: Features, applications and algorithms, Proceeding of the IEEE International Conference on Multimedia and Expo, pp 1013-1016.
6. Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography UsingReference Image. International Journal of Advancements in Technology , 1(1), pp.05.11 Bloom,J. A. et al.,2008.
7. Digital watermarking and Steganography .2nded. MorganKaufmann.Bishop, M., 2005.
8. Introduction to computer security.1sted.Pearson publications. 2nd Ed. Elsevier.Cummins, J. Diskin, P. Lau, S. &Parett, R., 2004.Steganography and digitalwatermarking