An Analysis of Key Dependent Image Steganography using Hybrid Edge Detection in Spatial Domain

Indu Maurya
Dept. of CSE, B.I.E.T Jhansi, Uttar Pradesh, India

Abstract
Steganography means hiding the fact that communication is taking place, by hiding information in some other information. Various carrier file formats can be used for this purpose, but digital images are the most popular. For hiding secret information or message in images, there is a large variety of steganographic techniques, in which, some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the technique used. In this paper, we are going to propose an improved secured Image Steganography scheme. This scheme uses the secret key based random LSB substitution. In this proposed work, Message to be embedded is first encrypted with AES (Advanced encryption standard) to provide another level of security then the encrypted message bits are hidden in the two areas: smooth area pixels and edge area pixels. For hiding the message bits in smooth area LSB substitution technique has been used. Whereas two components-based LSB Substitution techniques has been used for hiding message bits in the edge area and edges can bear more variation than smooth areas without being detected. This method ensures the higher PSNR value and high embedding capacity.

Keywords
Steganography, AES, Edge Detection, LSB Substitution; Peak Signal to Noise Ratio

I. Introduction
Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called Steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1] defining it as "covered writing". In image Steganography the information is hidden exclusively in images. Different steganographic techniques have been introduced since ancient times. Ancient techniques make use of invisible ink; microdots character arrangement etc. [2]. Due to digitization in modern times, digital media has become the source of Steganography e.g. images, text, audio and video files. Many other digital mediums are used for Steganography like floppy disk, hard drive, radio waves and network packet etc. [3]. Main goal of Steganography is to make the hidden information undetectable. Main components of image Steganography are as shown in the fig. 1.

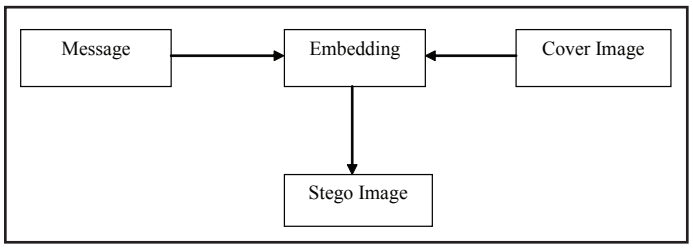

Fig. 1: Model of Steganography

Firstly both cover image and message bits are given as input to the embedding algorithm. An Embedding algorithm is a Steganography technique that will embed the message bits into the cover image such that intruder is unable to detect it. This algorithm will generate stego-image as an output. Stego image is the cover image containing message bits inside it. This image is communicated over the media between sender and receiver. At the receiver end an extraction algorithm will work on the stego image and extracts the hidden message bits from the stego image. There are three basic parameters for evaluation of different Steganography techniques.

A. Imperceptibility
It is the ability of Steganography method to avoid detection of hidden message through human visual system (HVS) and statistical analysis. It can be measured through peak signal to noise ratio (PSNR) [4].

B. Capacity
It is number of bits of message that are hidden into a stego image.

C. Robustness
It is ability of the Steganography technique to retain the hidden message after many image related operations. These operations are compression, cropping, rotation and filtering etc.

Two other technologies that are closely related to Steganography are watermarking and fingerprinting [5]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than Steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [6]. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [5].
In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it

may even be visible – while in Steganography the imperceptibility of the information is crucial [4]. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [5]. Research in Steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [7], forcing people to study other methods of secure information transfer. Businesses have also started to realise the potential of Steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [8]. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

II. Introduction to AES

Advanced Encryption Standard (AES) is the current standard for secret key encryption. AES was created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, replacing the old Data Encryption Standard (DES). The Federal Information Processing Standard 197 used a standardized version of the algorithm called Rijndael for the Advanced Encryption Standard. The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a MixColumn. It was successful because it was easy to implement and could run in a reasonable amount of time on a regular computer. Current alternatives to a new encryption standard were Triple DES (3DES) and International Data Encryption Algorithm (IDEA). The problem was IDEA and 3DES were too slow and IDEA was not free to implement due to patents. NIST wanted a free and easy to implement algorithm that would provide good security. Additionally they wanted the algorithm to be efficient and flexible. [31] After holding the contest for three years, NIST chose an algorithm created by two Belgian computer scientists, Vincent Rijmen and Joan Daemen. They named their algorithm Rijndael after themselves [31]. Supposedly Rijndael can only be pronounced correctly by people who can speak Dutch and the closest English approximation is "Rhine Dahl". [32] On November 26, 2001 the Federal Information Processing Standards Publication 197 announced a standardized form of the Rijndael algorithm as the new standard for encryption. This standard was called Advanced Encryption Standard and is currently still the standard for encryption.

Before applying the algorithm to the data, the block and key sizes must be determined. AES allows for block sizes of 128, 168, 192, 224, and 256 bits. AES allows key sizes of 128, 192, and 256 bits [31]. The standard encryption uses AES-128 where both the block and key size are 128 bits. The block size is commonly denoted as Nb and the key size is commonly denoted as N_k. N_b refers to the number of columns in the block where each row in the column consists of four cells of 8 bytes each for AES-128 [34]. The following example will show how data is broken up into blocks. Using AES-128 means that each block will consist of 128 bits. N_b can be calculated by dividing 128 by 32. The 32 comes from the number of bytes in each column. When the plain text data is stored into blocks and the key is chosen the Rijndael encryption algorithm can be applied. Some of the following steps could be done before the encryption process starts, but for simplicity they will be discussed when they are needed.

At a basic level the Rijndael algorithm uses a number of rounds to transform the data for each block. The number of rounds used is 6 + the maximum of N_b and N_k. Following from the previous example of AES-128, the number of rounds is 10. This is calculated from 6 plus the maximum of (4, 4). Since Nb and Nk are both 4, the number of rounds is 6 + 4 = 10 [31]. The initial block (also known as a state) is added to an expanded key derived from the initial cipher key. Then the round processing occurs consisting of operations of the S-box, shifts, and a MixColumn. The result state is then added to the next expanded key. This is done for all ten rounds, with the exception of the MixColumn operation of the final round. The final result is the encrypted cipher block. [34]

The original cipher key needs to be expanded from 16 bytes to 16(r + 1) bytes. In the example, there are ten rounds so r = 10. A round key is needed after each round and before the first round. Each round key needs to be 16 bytes because the block size is 16 bytes. Therefore, the cipher key needs to be expanded from 16 bytes to 16(r + 1) bytes or 176 bytes. The expanded key is then broken up into round keys. Round keys are added to the current state after each round and before the first round. The details on the key expansion algorithm are complex and will be skipped. [33]

Decryption is simple after understanding the encryption process. It is basically just the inverse. The algorithm was designed for all the steps to be invertible so decryption is basically like doing everything backwards. Therefore, for decryption starts at the last round and the last round key. When processing each round do the process backwards. So, the round key is added first to the last round. Addition is its own inverse, which is nice. Then the MixColumn step is applied. The MixColumn step is applied to all rounds except the last one. Also the inverse MixColumn table is used [34]. This table is generated with another matrix similar to the way the MixColumn table was generated. The difference is that there are no short cuts to generate the table.

III. Previous Work

The simplest way to hide information within the image is Least Significant Bit Substitution (LSB) technique .In this technique least significant bits of each pixel are replaced with the binary data (i.e. information) [9]. However this is not a secure technique as the stego image contains flecks at the place where the message bits are hidden and hidden message bits can easily be recovered through repetition of the same process. Many attacks like sample pair analysis [10], difference image histogram [11], blind detection algorithm [12] has been performed on this method. In order to overcome the problem of LSB substitution a new tool named "Hide and Seek for Windows 95" has been introduced. This tool distributes the information to be hidden randomly across the image pixels [13]. But drawback is that the information hidden using both these methods can be easily detected by the intruder. An attack can be performed on these two methods using Laplace formula [14]. In 2006 only, an adaptive filtering based image Steganography technique has been introduced. Adaptive Steganography takes into account human visual system's sensitivity and also statistical properties are taken under consideration to avoid steg analysis. The challenging issue in existing adaptive Steganography methods is that they don't specify any method to control the number of bits hidden in carrier medium [16-19] . In this technique data bits are hidden into the high intensity components and low intensity components are not used for hiding data. This method firstly passes the image to the filter to separate low and high intensity component. Then inverse transformation of both the images is performed after that data bits are embedded into High Frequency

Spatial Image (HFSI). Then combination of both HFSI and LFSI results into stego image. During embedding magnitude of the pixel is also considered. Higher the value of magnitude higher the number of bits embedded in that pixel [20]. In 2007, Random edge LSB (RELSB) technique has been introduced. This approach randomly hides the message bits into the regions that have least similarity with their neighbourhood. These regions generally contain edges, thin lines, end of lines etc. Robert cross gradient operator is used to extract such regions. Then random locations in these regions are selected using random number generator algorithm i.e. PRNG. The simplified data encryption standard (S-DES) is used to encrypt the message bits. Encryption is done to provide another layer of security. Data is hidden is such a way that same edges and line pixels are detected before and after data embedding. This approach has been better than LSB substitution [9], random LSB Embedding [13], edge LSB embedding [18]as gradient energy technique can detect number of hidden bits in all these three technique but not in RELSB[21]. In 2008 another edge based LSB Steganography technique has been introduced. This is based on Pixel Value Differencing (PVD) and LSB replacement [22] with some modification in these and provides more capacity and imperceptibility. The difference of a given pixel with its neighbour pixel is used to decide the embedding rate for that pixel. In this approach, firstly image is divided into non overlapping two consecutive blocks of size two. Then difference of two pixels into the blocks is calculated to categorize blocks into levels. In 2009 named as variable rate Steganography using neighbour pixel relationship. This technique also overcomes the drawback PVD technique [24] which also uses range table. The pixel's relationship with its neighbourhood is used to decide whether it is an edge pixel or smooth area pixel. On the basis of neighbourhood relationship three methods "four neighbours method", "diagonal neighbour method", "eight neighbour method" were given. All these methods have better Peak Signal to Noise Ratio (PSNR). But main drawback is that only half numbers of the pixels are used for embedding rather than using almost all pixels [25]. In 2011, a new edge embedding technique has been introduced that target on higher PSNR rather than higher embedding rate. This method provides better PSNR than [2, 23, 25]. Edges of the image are obtained using sobel/canny edge detector. Only horizontal edges of a particular edge length are used further. These edge pixels are used for embedding purpose but to calculate the difference of these edge pixels with upper edge boundary. If this difference is greater than some predefined difference then these upper boundary pixels are used for embedding data bits accordingly. In this way the stego image with least perceptual transparency is obtained. The strong point of this method is high PSNR value but having a drawback of least embedding capacity. In 2012, a new parameterized canny edge detection based embedding approach has been introduced. Parameterized canny edge detector uses three parameters i.e. higher threshold value, Gaussian filter and lower threshold value. The value of all these three parameters are user defined. This property makes the stego image more robust as different values of these parameters yields different outputs. In this approach three LSBs of all three channels of edge pixels are replaced with the secret data bits. The advantages of this approach are imperceptibility and irrecoverability [30]. In 2013, to improve the capacity and PSNR new LSB based edge embedding technique using hybrid edge detection filter. Rather than applying Canny with fuzzy edge detector as in [26] combination of the Canny and enhanced Hough edge detector is used to get edge pixels. Message to be embedded is encrypted with AES [30] to provide another level of security. The encrypted message bits are hidden in the smooth area pixels and edge area pixels. For hiding the message bits in smooth area adaptive LSB Substitution technique has been used. Whereas for hiding message bits in the edge area two components-based LSB Substitution techniques has been used. This method ensures the higher PSNR value and high embedding capacity.

IV. Proposed Method

The steps of the proposed methodology are as follows:

Step 1: Apply hybrid edge detection to obtain edge image B from gray scale image G.

Step 2: Applying AES encryption algorithm to get the encrypted secret image and divide the gray scale image into set of blocks, each block containing n-pixels. Here we use P1 pixel to store status of other pixel. If it is a edge pixel then the status of each pixel Pi, is defined as '1' Otherwise is '0' if non-edge pixel. The status of pixels from P2 to Pn is stored inside P1 by LSBs substitution operation.

Step 3: For a non edge pixel in a block we embed 'y' bits of message XOR with 'y' MSBs of the pixel by LSB substitution.

Step 4: For an edge pixel in a block, we embed 'x' bits of message XOR with 'x' MSBs of the pixel by LSB substitution. The value of 'x' is generated randomly for each pixel using chaotic map.

The steps of extraction process are as follows.

Step 1: Similar to the dividing operation presented in the previous procedure. Applying AES decryption algorithm and extract the original image and divide the stego image into n pixels block.

Step 2: Based on the (n - 1) LSBs in pixel P1', we obtain the status of the remaining pixels from P2' to P_n'. From this status value, we can identify two categories corresponding to the non-edge pixel category and the edge pixels category.

Step 3: From non-edge pixel, based on the value of 'y' used in embedding process, extract the 'y' LSBs of the pixel and XOR it with the 'y' MSBs of the pixel to obtain the bits of original message.

Step 4: From edge pixel, based on the value of 'x' generated randomly, extract 'x' LSBs of the pixel and XOR it with the 'x' MSBs of the pixel to achieve part of message. The value of 'x' generated will be same for a pixel in embedding & extraction.

V. Conclusion

Steganography is an important field of information security and digital image processing. Various Steganography techniques introduced to provide high Imperceptibility, robustness and capacity. Initially LSB substitution technique was used. This Improvement in PSNR and embedding capacity can be achieved and improved by using hybrid approach rather than using single approach. More over better edge detectors can be used to have more number of edge pixels that can be used for embedding. In this paper, we have proposed an improved key dependant image Steganography scheme which is based on random LSB Steganography with hybrid edge detection. Moreover, because we are using random and encrypted scheme for LSB Steganography, so the scheme is robust to attack and message cannot be recovered

without knowing the key. These techniques can also be combined with many cryptography techniques to improve security.

References

[1] Moerland, T.,"Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, http://www.liacs.nl/home/ tmoerl/privtech.pdf.

[2] Anderson R. J.,"Stretching the Limits of Steganography," Springer Lecture Notes in Computer Science, Vol. 1174, pp. 39–48, 1996.

[3] Westfeld A, J. Camenisch et al.,"Steganography for Radio Amateurs— A DSSS Based Approach for Slow Scan Television", Springer-Verlag Berlin Heidelberg, pp. 201-215, 2007.

[4] A. Shaddad, J. Condell, K. Curran, P. Mckevtt.,"Biometric inspired digital image steganography," Proceedings of 2008 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, pp. 159-168, 2008.

[5] Anderson, R.J., Petitcolas, F.A.P.,"On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[7] Marvel, L.M., Boncelet Jr., C.G., Retter, C.,"Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999.

[8] Dunbar, B.,"Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002.

[9] Artz, D.,"Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.

[10] Thien, C. C., Lin, J. C.,"A Simple and High-Hiding Capacity Method for Hiding Digit-By-Digit Data in Images Based On Modulus Function", Pattern Recognition, Vol. 36, No. 12, pp. 2875-2881, June 2003.

[11] S. Dumitrescu, X. Wu, Z. Wang,"Detection of LSB Steganography via Sample Pair Analysis", Proceedings of 2003 IEEE Transaction on Signal, Vol. 51, No. 7, pp. 1995-2007, 2003.

[12] T. Zhang, X. Ping,"Reliable detection of LSB steganography based on the difference histogram", IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 3, pp. 545-548, April 2003.

[13] L. Zhi, S. A. Fen, Y. Y. Xian,"A LSB steganography detection algorithm", Proc. of IEEE Symposium on Personal Indoor and Mobile Radio Communication, pp. 2780-2783, September 2003.

[14] Maroney, C. Hide, Seek 5 for Windows 95, computer software and documentation, originally released in Finland and the UK.

[15] Katzenbeisser. S, Fabien, Petitcolas. A.P., "Information hiding techniques for steganography and digital watermarking", Artech House, Norwood, MA 02062, USA, 1999.

[16] Kathryn Hempstalk,"Hiding Behind Corners: Using Edges in Images for Better Steganography", Proceedings of the Computing Women's Congress, 2006.

[17] R. Chandramouli, N.D. Memon, G. Li,"Adaptive Steganography," Proceedings on Security and Watermarking of Multimedia Contents III, Special session on Steganalysis, SPIE Photonics West, Vol. 4675, pp. 69-78, April 2002.

[18] Karen Bailey, Kevin Curran, Joan Condell,"An Evaluation of Pixel based Steganography and Stego detection Methods," The Imaging Science Journal, Vol. 52, No. 3, pp. 131 - 150, Sept 2004.

[19] Elke Franz, Antje Schneidewind,"Adaptive Steganography Based on Dithering," Proceedings of the 2004 workshop on multimedia and security, ACM, pp. 56-62, 2004.

[20] M. M. Amin, M. Salleh, S. Ibrahim, M. R. K.Atmin, M. Z. I. Shamsuddin,"Information Hiding using Steganography," 4th national Conference on Telecommunication Technology, NCTT 2003, IEEE, pp. 21 – 25, Jan 2003

[21] Santosh Arjun, N., Atul Negi,"A Filtering Based Approach to Adaptive Steganography," 10th Conference, TENCON 2006, IEEE, pp. 1-4, Nov 2006.

[22] Manglem Singh, Birendra Singh, Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images," IJCSNS, Vol. 7, No. 4, April 2007.

[23] H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Hwang,"Image steganographic scheme based on pixel-value differencing and LSB replacement methods," Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, Vol. 152, No. 5 pp. 611–615, 2005.

[24] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, pp. 488-497, 2008.

[25] D. C. Wu, W. H. Tsai,"A Steganographic method for images using pixel value differencing," Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.

[26] Hossain, M. Al Haque, S. Sharmin, F.,"Variable rate Steganography in gray scale digital images using neighborhood pixel," 12th International Conference Dhaka, Information Computers and Information Technology, ICCIT '09, pp. 267- 272, Dec 2009.

[27] Wen-Jan Chen a, Chin-Chen Chang, T. Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector," Expert Systems with Applications, Vol. 37, pp. 3292–3301, 2010.

[28] Sonka, M., Hlavac, V., Boyle,"Image processing, analysis, and machine vision", Thomson Brooks/ Cole, 1999.

[29] Hussain, M., Hussain,"Embedding data in edge boundaries with high PSNR," Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp. 1-6, Sept 2011.

[30] Youssef Bassil,"Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," International.

[31] Kaufman, C., Perlman, R., Speciner, M. Network Security: Private Communication in a Public World. 2nd ed. Upper Saddle River, N.J.: Prentice Hall PTR, 2002.

[32] Rijndael. Knowledgerush. 2009. [Online] Available:http://www.easybib.com/cite/form/website (accessed March, 15, 2010).

[33] Advanced Encryption Standard (AES). FIPS. November 23, 2001. [Online] Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[34] Daemen, J., Rijmen, V. AES Proposal: Rijndael. September 3, 1999. [Online] Available: http://www.comms.scitech.sussex.ac.uk/fft/crypto/rijndael.pdf